Publication 1075

Tax Information Security Guidelines For Federal, State and Local Agencies

Safeguards for Protecting Federal Tax Returns and Return Information

IRS Mission Statement

Provide America's taxpayers top-quality service by helping them understand and meet their tax responsibilities and enforce the law with integrity and fairness to all.

Office of Safeguards Mission Statement

The Mission of the Office of Safeguards is to promote taxpayer confidence in the integrity of the tax system by ensuring the confidentiality of IRS information provided to federal, state, and local agencies. Safeguards verifies compliance with IRC 6103(p)(4) safeguard requirements through the identification and mitigation of any risk of loss, breach, or misuse of Federal Tax Information held by external government agencies.

Changes for September 2016 Revision

This publication revises and supersedes Publication 1075 (October 2014) and is effective September 30, 2016. Feedback for Publication 1075 is highly encouraged. Please send any comments to SafeguardReports@irs.gov. Following are the highlighted changes:

1) Editorial changes have been made throughout this document to update website references and links, as well as to renumber sections and to clarify guidance

2) Table of Contents updated. Please find "tables" listed under respective sections rather than at the end of the *Table of Contents*

3) Section 1.3 – "Access Safeguards Resources Online" changed to "Access Safeguard Resources"

4) Section 1.3.1 – Added "Website Resources"

5) Section 1.3.2 – Added "Mailbox"

6) Section 1.4.1 – "Federal Tax Information (FTI)" – Added reference to include the Centers for Medicare and Medicaid and IRC 6103(p)(2)(B) Agreements

7) Section 2.7 – Created Section 2.7.1 "On-Site Review Process" and 2.7.2 "Computer Security Review" to elaborate on the Safeguard Review Process

8) Section 2.9 – Added "Voluntary Termination of Receipt of FTI"

9) Section 2.9.1 – Added "Archiving FTI"

10) Section 2.9.2 – Added "Termination Documentation"

11) Section 3.2 – Updated "Electronic and Non-Electronic Logs" requirements and deleted duplicate log sample

12) Section 4.4 – Deleted duplicate paragraph for FTI in transit

13) Section 4.6 – "Offsite Storage Requirements" – Updated to show agency-type specific requirements

14) Section 4.7.1 – "Equipment" - Added exception for use of VDI and updated to include personally-owned devices

15) Section 5.1.1 – Added "Background Investigation Minimum Requirements"

16) Section 5.4.2 – Added guidance for use of Consolidated Data Centers

17) Section 5.4.2.1 – Added all contractor and shared sites to be included in Safeguard reviews

18) Section 5.4.3 – Added “Review Availability of Contractor Facilities”

19) Section 6.3 – Updated “Disclosure Awareness Training”

20) Section 7.2.1 – Renamed from “SSR Update Submission and Instructions” to “Initial SSR Submission Instructions-New Agency Responsibility”

21) Section 7.2.2 – Renamed from “SSR Update Submission Dates” to “Instructions for Agencies Requesting New FTI Data Streams” and includes the mandatory requirement for providing evidence of security testing and ATO before the system is operational

22) Section 7.2.3 – Renamed from “SSR Update Submission Instruction” to “Annual SSR Update Submission Instructions”

23) Section 7.2.2 – Renumbered “SSR Update Submission Dates” to Section 7.2.4

24) Section 7.4 – Added table for 45 Day Notification Reporting Requirements

25) Section 7.4.4 – Removed requirement to notify Safeguards prior to implementing a data warehouse

26) Section 7.4.5 – “Non-Agency Owned Systems” updated

27) Section 7.4.8 – Removed requirement to notify Safeguards prior to locating FTI in a virtual environment

28) Section 8.3 – “Destruction and Disposal” – Updated section to include new requirements regarding shredding and updated regarding whenever physical media leaves the physical or systemic control of the agency

29) Section 9.2 – Updated Table 8 for Automated Compliance and Vulnerability Assessment Testing to include profiles used with these tools can be downloaded from the Office of Safeguards’ website

30) Section 9.3.1.7(b) – “Unsuccessful Log On Attempts (AC-7) - Updated automatic lock period to 15 minutes

31) Section 9.3.1.10 – “Session Termination (AC-12)” – Updated to show information system must automatically terminate a user session after 30 minutes of inactivity

32) Section 9.3.1.15 – “Use of External Information Systems (AC-20) – Updated to reflect personally-owned device requirements.

33) Section 9.3.2.3 – Added definition of personnel with security roles and responsibilities and added distinction from Section 6.3, Disclosure Awareness and 9.3.2.2, Security Awareness Training (AT-2)

34) Section 9.3.3.8(c) – “Time Stamps (AU-8)” – Updated regarding synchronization of internal information system clocks

35) Section 9.3.3.10 – “Audit Record Retention (AU-11)” – Added clarification on retention

36) Section 9.3.7.3 – “Device Identification and Authentication (IA-3)” – Added clarification

37) Section 9.3.8.3 – Updated Incident Response Testing to remove the word, “systems” as testing requirements apply to both paper and electronic FTI

38) Section 9.3.11.7 – Updated to reflect 5 year retention period requirement

39) Section 9.3.12.3(c) – Added to Rules of Behavior (PL-4), “review and update at a minimum annually”

40) Section 9.3.15.6 – “Security Engineering Principles” (SA-8) - Added clarification of what security engineering principles include

41) Section 9.4.8 – “Mobile Devices ” - Updated to reflect current restrictions with BYOD

42) Section 9.4.9 – Updated Multi-Functional Devices to include High-Volume Printers

43) Section 9.4.11(g) – “Storage Area Networks” - changed audit review to weekly

44) Section 9.4.13 – “Virtual Desktop Infrastructure” – updated to include agency and non-agency owned requirements

45) Section 9.4.14 – “Virtual Environment” Removed requirement to notify Safeguards prior to locating FTI in a virtual environment

46) Section 9.4.17 – “Web Browser” – Removed requirement a) Private browsing must be enabled on the Web browser and configured to delete temporary files and cookies upon exiting the session

47) Section 10.0 – Updated Reporting Improper Inspections or Disclosures including Table 9: TIGTA Field Division Contact Information

48) Section 12.1 – Updated guidelines for agencies authorized to produce statistical reports in “Return Information in Statistical Reports – General”

49) Exhibit 7 – “Safeguarding Contract Language” - added additional requirements in Section I Performance and Section III Inspection

50) Exhibit 10 – Changed to reflect updated SSR Requirements

51) Exhibit 12 – *Glossary and Terms* is no longer labeled, but is still found in the back of the publication

Table of Contents

1.0 Introduction 1

1.1 General 1

1.2 Overview of Publication 1075 2

1.3 Access Safeguards Resources 3

1.3.1 Website Resources 3

1.3.2 Mailbox 3

1.4 Key Definitions 4

1.4.1 Federal Tax Information (FTI) 4

1.4.2 Return and Return Information 4

1.4.3 Personally Identifiable Information 5

1.4.4 Information Received From Taxpayers or Third Parties 5

1.4.5 Unauthorized Access 6

1.4.6 Unauthorized Disclosure 6

1.4.7 Need to Know 6

2.0 Federal Tax Information and Reviews 7

2.1 General 7

2.2 Authorized Use of FTI 8

2.3 Secure Data Transfer 8

2.4 State Tax Agency Limitations 8

2.5 Coordinating Safeguards within an Agency 10

2.6 Safeguard Reviews 10

2.7 Conducting the Review 10

Table 1 – Safeguard Review Cycle 11

2.7.2 Computer Security Review Process 12

Table 2 – IT Testing Techniques 13

2.8 Corrective Action Plan 13

2.9 Voluntary Termination of Receipt of FTI 14

2.9.1 Termination Documentation 14

2.9.2 Archiving FTI Procedure (for agencies terminating receipt of FTI but required by statute to retain FTI for designated periods) 14

3.0 Recordkeeping Requirement 15

3.1 General 15

3.2 Electronic and Non-Electronic FTI Logs 15

Figure 1 – Sample FTI Log 16

3.3 Converted Media *16*
3.4 Recordkeeping of Disclosures to State Auditors *16*
4.0 Secure Storage—IRC 6103(p)(4)(B) *17*
4.1 General *17*
4.2 Minimum Protection Standards *17*
Table 3 – Minimum Protection Standards *18*
4.3 Restricted Area Access *19*
Figure 2 – Sample Visitor Access Log *20*
4.3.1 Use of Authorized Access List *20*
4.3.2 Controlling Access to Areas Containing FTI *21*
4.3.3 Control and Safeguarding Keys and Combinations *21*
4.3.4 Locking Systems for Secured Areas *22*
4.4 FTI in Transit *22*
4.5 Physical Security of Computers, Electronic, and Removable Media *23*
4.6 Media Off-Site Storage Requirements *23*
4.7 Telework Locations *24*
4.7.1 Equipment *24*
4.7.2 Storing Data *25*
4.7.3 Other Safeguards *25*
5.0 Restricting Access—IRC 6103(p)(4)(C) *26*
5.1 General *26*
5.1.1 Background Investigation Minimum Requirements *26*
5.1.2 Implementing the Background Investigation Requirement *28*
5.2 Commingling of FTI *29*
5.2.1 Commingling of Electronic Media *29*
5.3 Access to FTI via State Tax Files or Through Other Agencies *30*
5.4 Controls over Processing *31*
5.4.1 Agency Owned and Operated Facility *31*
5.4.2 Contractor or Agency Shared Facility - Consolidated Data Centers *31*
5.4.2.1 Agency Shared Facilities: *31*
5.4.2.2 Consolidated Data Centers: *32*
5.4.3 Review Availability of Contractor Facilities: *33*
5.5 Child Support Agencies—IRC 6103(l)(6), (l)(8), and (l)(10) *34*
5.6 Human Services Agencies—IRC 6103(l)(7) *34*
5.7 Deficit Reduction Agencies—IRC 6103(l)(10) *34*

5.8 Centers for Medicare and Medicaid Services—IRC 6103(l)(12)(C) 35
5.9 Disclosures under IRC 6103(l)(20) 35
5.10 Disclosures under IRC 6103(l)(21) 35
5.11 Disclosures under IRC 6103(i) 35
5.12 Disclosures under IRC 6103(m)(2) 36
6.0 Other Safeguards—IRC 6103(p)(4)(D) 37
6.1 General 37
6.2 Training Requirements 37
Table 4 – Training Requirements 37
6.3 Disclosure Awareness Training 38
6.3.1 Disclosure Awareness Training Products 39
6.4 Internal Inspections 40
6.4.1 Recordkeeping 40
6.4.2 Secure Storage 40
6.4.3 Limited Access 41
6.4.4 Disposal 41
6.4.5 Computer Systems Security 41
6.5 Plan of Action and Milestones 41
7.0 Reporting Requirements—6103(p)(4)(E) 42
7.1 General 42
7.1.1 Report Submission Instructions 42
7.1.2 Encryption Requirements 43
7.2 Safeguard Security Reports 43
7.2.1 Initial SSR Submission Instructions – New Agency Responsibilities 43
Table 5 - Evidentiary Requirements for SSR approval before release of FTI 44
7.2.2 Agencies Requesting New FTI Data Streams 46
7.2.3 Annual SSR Update Submission Instructions 46
7.2.4 SSR Update Submission Dates 47
Table 6 – SSR Due Dates 47
7.3 Corrective Action Plan 48
7.3.1 CAP Submission Instructions and Submission Dates 48
Table 7 – CAP Due Dates 48
7.4 45-Day Notification Reporting Requirements 50
Table 8 – 45-Day Notification Reporting Requirements 50
7.4.1 Cloud Computing 51

7.4.2 Consolidated Data Center *51*
7.4.3 Contractor or Subcontractor Access *51*
7.4.4 Data Warehouse Processing *51*
7.4.5 Non-Agency-Owned Information Systems *51*
7.4.6 Tax Modeling *52*
7.4.7 Live Data Testing *52*
7.4.8 Virtualization of Information Technology Systems *52*
8.0 Disposing of FTI—IRC 6103(p)(4)(F) *53*
8.1 General *53*
8.2 Returning IRS Information to the Source *53*
8.3 Destruction and Disposal *53*
Table 9 – FTI Destruction Methods *53*
8.4 Other Precautions *54*
9.0 Computer System Security *55*
9.1 General *55*
9.2 Assessment Process *55*
9.3 NIST SP 800-53 Control Requirements *56*
9.3.1 Access Control *56*
9.3.2 Awareness and Training *62*
9.3.3 Audit and Accountability *63*
Table 10 – Proactive Auditing Methods to Detect Unauthorized Access to FTI *66*
9.3.4 Security Assessment and Authorization *68*
9.3.5 Configuration Management *70*
9.3.6 Contingency Planning *74*
9.3.7 Identification and Authentication *76*
9.3.8 Incident Response *79*
9.3.9 Maintenance *81*
9.3.10 Media Protection *83*
9.3.11 Physical and Environmental Protection *85*
9.3.12 Planning *88*
9.3.13 Personnel Security *89*
9.3.14 Risk Assessment *91*
9.3.15 System and Services Acquisition *93*
9.3.16 System and Communications Protection *96*
9.3.17 System and Information Integrity *101*

9.3.18 Program Management *105*
9.4 Additional Computer Security Requirements *105*
9.4.1 Cloud Computing Environments *105*
9.4.2 Data Warehouse *107*
9.4.3 Email Communications *108*
9.4.4 Fax Equipment *108*
9.4.5 Integrated Voice Response Systems *109*
9.4.6 Live Data Testing *109*
9.4.7 Media Sanitization *110*
9.4.8 Mobile Devices *111*
9.4.9 Multi-Functional Devices and High Volume Printers *112*
9.4.10 Network Protections *113*
9.4.11 Storage Area Networks *113*
9.4.12 System Component Inventory *114*
9.4.13 Virtual Desktop Infrastructure *115*
9.4.14 Virtualization Environments *116*
9.4.15 VoIP Systems *117*
9.4.16 Web-Based Systems *117*
9.4.17 Web Browser *118*
9.4.18 Wireless Networks *119*
10.0 Reporting Improper Inspections or Disclosures *120*
10.1 General *120*
Table 11 – TIGTA Field Division Contact Information *120*
10.2 Office of Safeguards Notification Process *121*
10.3 Incident Response Procedures *122*
10.4 Incident Response Notification to Impacted Individuals *122*
10.5 FTI Suspension, Termination, and Administrative Review *122*
11.0 Disclosure to Other Persons *123*
11.1 General *123*
11.2 Authorized Disclosure Precautions *123*
11.3 Disclosing FTI to Contractors *124*
11.4 Re-Disclosure Agreements *124*
12.0 Return Information in Statistical Reports *125*
12.1 General *125*
12.2 Making a Request under IRC 6103(j) *125*

12.3 State Tax Agency Statistical Analysis *126*
12.4 Making a Request under IRC 6108 ..... *126*
Exhibit 1 USC Title 26, IRC 6103(a) and (b) *127*
Exhibit 2 USC Title 26, IRC 6103(p)(4) *131*
Exhibit 3 USC Title 26, CFR 301.6103(p)(7)-1 ..... *133*
Exhibit 4 Sanctions for Unauthorized Disclosure *135*
Exhibit 5 Civil Damages for Unauthorized Disclosure *137*
Exhibit 6 Contractor 45-Day Notification Procedures *139*
Exhibit 7 Safeguarding Contract Language *141*
Exhibit 8 Warning Banner Examples *142*
Exhibit 9 Record Retention Schedules *143*
Table 12 – Record Retention Schedules *143*
Exhibit 10 Data Warehouse Security Requirements *145*
Exhibit 11 Media Sanitization Techniques *152*
Table 13 – Media Sanitization Techniques *152*
Glossary and Key Terms *154*

1.0 Introduction

1.1 General

To foster a tax system based on voluntary compliance, the public must maintain a high degree of confidence that the personal and financial information furnished to the Internal Revenue Service (IRS) is protected against unauthorized use, inspection, or disclosure.

The IRS must administer the disclosure provisions of the Internal Revenue Code (IRC) according to the spirit and intent of these laws, ever mindful of the public trust. The IRC defines and protects the confidential relationship between the taxpayer and the IRS and makes it a crime to violate this confidence. IRC 7213 prescribes criminal penalties, making it a felony offense for federal and state employees and others who illegally disclose federal tax returns and return information. Additionally, IRC 7213A makes the unauthorized inspection of Federal Tax Information (FTI) a misdemeanor, punishable by fines, imprisonment, or both. And finally, IRC 7431 prescribes civil damages for unauthorized inspection or disclosure, and upon criminal indictment or information under IRC 7213 or 7213(A), notification to the taxpayer that an unauthorized inspection or disclosure has occurred.

The concerns of citizens and Congress regarding individual rights to privacy require the IRS to continuously assess disclosure practices and the safeguards used to protect the confidential information entrusted. While the sanctions of the IRC are designed to protect the privacy of taxpayers, the IRS recognizes the importance of cooperating to the fullest extent permitted by law with other federal, state, and local authorities in their administration and enforcement of laws.

Those agencies or agents that legally receive FTI directly from either the IRS or from secondary sources (e.g., Social Security Administration [SSA]), pursuant to IRC 6103 or by an IRS-approved exchange agreement must have adequate programs in place to protect the data received. Furthermore, as agencies procure contractor services, it becomes equally important that contractors protect that information from unauthorized use, access, and disclosure.

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

Release of any IRS Safeguards document requires the express permission of the Internal Revenue Service. Requests received through Sunshine and/or Information Sharing/Open Records provisions must be referred to the federal Freedom of Information Act (FOIA) statute for processing. State and local agencies receiving such requests should refer the requestor to the instructions to file a FOIA request with the IRS. Federal agencies should follow established procedures which require consultation before citing FOIA exemptions on IRS agency records, or directly refer the FOIA request to IRS for processing.

The intent of this requirement is to address any public request for sensitive information and prevent disclosure of data that would put FTI at risk. The agency may still distribute these reports internally and within other state agencies, auditors or oversight panels as required to either take corrective actions or report status without further IRS approval.

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

1.2 Overview of Publication 1075

This publication provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of FTI.

Enterprise security policies address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to implement all applicable security controls. This document contains the managerial, operational, and technical security controls that must be implemented as a condition of receipt of FTI.

The guidelines outlined herein apply to all FTI, no matter the amount or the media in which it is recorded. FTI must be afforded the same levels of protection regardless of it residing on paper or electronic form. Systematic, procedural, or manual security policies must minimize circumvention.

A mutual interest exists in our responsibility to ensure that FTI is disclosed only to persons authorized and used only as authorized by statute or regulation. The IRS is confident of your diligence in this area and believes that this publication will be a helpful resource.

Conforming to these guidelines meets the safeguard requirements of IRC 6103(p)(4) and makes our joint efforts beneficial.

Requirements throughout this document apply to all organizational segments of an agency receiving FTI. It is the agency's responsibility to ensure all functions within the agency, including consolidated data centers and contractors (where allowed by federal statute) with access to FTI, understand and implement the requirements in this publication.

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

The Office of Safeguards is responsible for all interpretations of safeguarding requirements. Publication 1075 requirements may be supplemented or modified between editions of Publication 1075 via guidance issued by the Office of Safeguards and posted on the Office of Safeguards website.

1.3 Access Safeguards Resources

The Office of Safeguards maintains Publication 1075, templates, guidance, and frequently asked questions online at http://www.irs.gov/uac/Safeguards-Program. Agencies are highly encouraged to regularly visit the website for updates.

1.3.1 Website Resources

The website contains many resources to assist agencies with meeting Publication1075 requirements. Examples of the website's features include:

- Safeguard alerts and technical assistance memorandums
- Recommendations on how to comply with Publication 1075 requirements
- Reporting requirement templates (e.g., Safeguard Security Report [SSR]) and guidance
- Instructions for reporting unauthorized accesses, disclosures, or data breaches
- Internal inspections report templates and instructions
- IRS disclosure awareness videos and resources
- Disclosure and physical security requirements documented in the Safeguard Disclosure Security Evaluation Matrix (SDSEM) template
- Computer security requirements documented in Safeguard Computer Security Evaluation Matrix (SCSEM) templates organized by technology or topic

1.3.2 Mailbox

The Safeguards Mailbox is a repository for information and communication to the Office of Safeguards relative to Safeguarding requirements and Publication 1075. The Mailbox is located at SafeguardReports@irs.gov. Below are items that are appropriate for submission to the Mailbox:

- Safeguards Reports and Extension Requests
- 45 Day Notifications
- Publication 1075 Technical Inquiries
- Re-Disclosure Agreements

1.4 Key Definitions

This section establishes a baseline of key terms used throughout this publication. For additional definitions of terms and phrases, refer to *Glossary and Key Terms*.

1.4.1 Federal Tax Information (FTI)

Safeguarding FTI is *critically important* to continuously protect taxpayer confidentiality as required by IRC 6103. FTI is a term of art and consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the confidentiality protections of the IRC and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI is categorized as Sensitive But Unclassified information and may contain personally identifiable information (PII).

FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement.

FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

> FTI may not be masked to change the character of information to circumvent IRC 6103 confidentiality requirements.

1.4.2 Return and Return Information

IRC 6103(b)(1) defines a return as 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. Examples of returns include forms filed on paper or electronically, such as Forms 1040, 941, 1120, and other informational forms, such as 1099 or W-2[*]. Forms include supporting schedules, attachments, or lists that are supplemental to or part of such a return.

[*] Refer to IRS.gov for a complete catalog of IRS forms.

Return information, in general, is 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. It includes but is not limited to:

- Information that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture, or other imposition or offense
- Information extracted from a return, including names of dependents or the location of business
- The taxpayer's name, address, and identification number
- Information collected by the IRS about any person's tax affairs, even if identifiers, such as name, address, and identification number are deleted
- Status of whether a return was filed, under examination, or subject to other investigation or processing, including collection activities
- Information contained on transcripts of accounts

1.4.3 Personally Identifiable Information

FTI may include Personally Identifiable Information (PII). FTI may include the following PII elements:

- Name of a person with respect to whom a return is filed
- Taxpayer mailing address
- Taxpayer identification number
- E-mail addresses
- Telephone numbers
- Social Security Numbers
- Bank account numbers
- Date and place of birth
- Mother's maiden name
- Biometric data (e.g., height, weight, eye color, fingerprints)
- Any combination of the above

1.4.4 Information Received From Taxpayers or Third Parties

Copies of tax returns or return information provided to the agency directly by the taxpayer or his/her representative (e.g. W-2's, Form 1040, etc.) or obtained from public information files (e.g. federal tax lien on file with the county clerk, Offers in Compromise available for public inspection; court records, etc.) is not protected FTI that is subject to the safeguarding requirements of IRC 6103(p)(4). If the agency independently verifies FTI provided by the IRS or a secondary source *with the* taxpayer or a third party source, the verified information is not FTI as long as the IRS source information is replaced or overwritten with the newly provided information.

1.4.5 Unauthorized Access

Unauthorized access occurs when an entity or individual knowingly or due to gross negligence receives or has access to FTI without authority, as defined in IRC 6103.

> *Access to FTI is permitted only to individuals who require the FTI to perform their official duties and as authorized under the IRC. FTI must never be indiscriminately disseminated, even within the recipient agency, body, or commission. Agencies must evaluate the need for FTI before the data is requested or disseminated.*

1.4.6 Unauthorized Disclosure

An unauthorized disclosure occurs when an entity or individual with authorization to receive FTI knowingly or with gross negligence discloses FTI to another entity or individual who does not have authority, as defined in IRC 6103 and IRC 6104(c).

> *An unauthorized disclosure has occurred when FTI is knowingly or due to gross negligence provided to an individual who does not have the statutory right to have access to it under the IRC. Even without willfulness or gross negligence FTI is not to be disclosed to entities or individuals who are not authorized by IRC 6103 to have it.*

Subject to the disclosure provisions of IRC 6103, agencies may need to disclose FTI to outside entities (e.g., for prosecution, appeals, or collection processes) as long as the receiving entity has a need-to-know and the individual recipient has authority under IRC 6103 to receive it. If the individual does not have a need-to-know, this constitutes an unauthorized disclosure.

1.4.7 Need to Know

Under need-to-know restrictions, even if an entity or an individual has the authority to access FTI, one would not be given access to such information if it were not necessary to perform his or her official duties with regard to the purpose for which IRC 6103 provides the FTI is to be used.

> *Limiting access to individuals on a need-to-know basis reduces opportunities to "browse" or improperly view FTI. Restricting access to designated personnel minimizes improper access or disclosure. When FTI must be provided to clerical, computer operators, or others, these should only be provided the FTI that is essential to accomplish their official duties.*

2.0 Federal Tax Information and Reviews

2.1 General

IRC 6103 is a confidentiality statute and generally prohibits the disclosure of FTI (see *Exhibit 1, USC Title 26, IRC 6103,* for general rules and definitions). Exceptions to the general rule authorize disclosure of FTI to certain federal, state, and local agencies. Generally, these disclosures are made by the IRS in response to written requests signed by the head of the requesting agency or an authorized delegate. FTI so disclosed may be used by the receiving agency solely for the purpose described in the exception authorizing the disclosure. The statutes providing authorization to disclose FTI contain specific conditions that may require different procedures in maintaining and using the information. These conditions are outlined under specific sections in this publication.

As a condition of receiving FTI, the receiving agency must show, to the satisfaction of the IRS, the ability to protect the confidentiality of that information. Certain safeguards must be implemented to prevent unauthorized access and use. Besides written requests, the IRS may require formal agreements that specify, among other things, how the information will be protected. An agency must ensure its safeguards will be ready for immediate implementation upon receipt of FTI. Copies of the initial and subsequent requests for data and any formal agreement must be retained by the agency a minimum of five years as a part of its recordkeeping system.

Agencies must always maintain the latest SSR on file. The initial request for FTI must be followed by submitting an SSR to the IRS at least 45 days before the scheduled or requested receipt of FTI (see *Section 7.0, Reporting Requirements—6103(p)(4)(E)*). The SSR must include processing and safeguard procedures for all FTI received and distinguish between agency programs and functional organizations using FTI. Multiple organizations, divisions or programs within a federal agency using FTI should be consolidated into a single report for that agency at the direction of the Office of Safeguards.

Agencies entering into an agreement to disclose FTI to agents or contractors requires advance notice to the Office of Safeguards (see *Section 7.4, 45 Day Notification Reporting Requirements* and *Section 11.3, Disclosing FTI to Contractors.*)

> *Agencies must exercise care in outlining their safeguard program. Reports that lack clarity or sufficient information will be returned to the submitting agency for additional documentation.*

2.2 Authorized Use of FTI

Any agency that receives FTI for an authorized use may not use that information in any manner or for any purpose not consistent with that authorized use. If an agency needs FTI for a different authorized use under a different provision of IRC 6103, a separate request must be sent to the Office of Disclosure.

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

The Office of Safeguards conducts "need and use" verification reviews as part of the safeguard review and always considers whether the agency's use is in conformance with the governing provisions allowing the disclosure of FTI. The agency must describe the purpose(s) for which FTI is collected, used, maintained, and shared.

2.3 Secure Data Transfer

The IRS established a Secure Data Transfer (SDT) program to provide encrypted electronic transmission of FTI between the IRS and trading partners. For support with establishing an IRS SDT account, please submit an SDT Customer Support Request. Complete information on establishing an SDT account is available in the SDT Handbook. The SDT Handbook is available from a local IRS governmental liaison or a request to the Safeguards mailbox.

In addition to installing the SDT software, each agency must also have an IdenTrust Certificate installed. After the initial installation, agencies are required to renew the IdenTrust Certificate every two years. Refer to the ACES (Access Certificates for Electronic Services) IdenTrust website for additional information.

Only the following types of documents will be accepted via SDT:

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

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

2.4 State Tax Agency Limitations

FTI may be obtained per IRC 6103(d) by state tax agencies only to the extent the information is needed for, and is reasonably expected to be used for, state tax administration. An agency's records must include some account of the result of its use of FTI (e.g., disposition of closed cases and summary of revenues generated) or

include reasons why the information was not used. If any agency continually receives FTI that it is unable to use for any reason, it must contact the IRS official liaison and discuss the need to stop the receipt of this FTI.

State tax agencies using FTI to conduct statistical analysis, tax modeling, or revenue projections must notify the IRS by submitting a signed *Need and Use Justification for Use of Federal Tax Information* form and following the established guidelines.

Annually, the agency must provide updated information in the SSR regarding its modeling activities that include FTI. In the SSR, the agency must describe:

- Any use of FTI that is in addition to what was described in the original Need and Use Justification Form
- Any new, previously unreported internal tax administration compilations that include FTI
- Changes to the listing of authorized employees (Attachment B to the Need and Use Justification Form)

If the agency intends to use a contractor for conducting statistical analysis, tax modeling, or revenue projections, it must submit a 45-day notification (see *Section 11.3, Disclosing FTI to Contractors*) prior to contractor access to the FTI. The agency's SSR must detail the use of FTI for this purpose. In addition, the agency must submit a separate statement detailing the methodology used and data to be used by the contractor. The Office of Safeguards and Statistics of Income functions will review the information provided to confirm that appropriate safeguarding protocols are in place and that the modeling methodology to be used to remove taxpayer identifying information is appropriate.

The agency must:

a) Identify the minimum FTI elements (e.g., name, address, date of birth) that are relevant and necessary to accomplish the legally authorized purpose of collection
b) Limit the collection and retention of FTI to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent
c) Conduct an initial evaluation of FTI holdings, as well as:

    i. Establish and follow a schedule for regularly reviewing those holdings to ensure that only FTI identified in the notice is collected and retained; and
    ii. Certify that the FTI continues to be necessary to accomplish the legally authorized purpose.

2.5 Coordinating Safeguards within an Agency

Because of the diverse purposes that authorized disclosures may be made to an agency and the division of responsibilities among different components of an agency, FTI may be received and used by several quasi-independent units within the agency's organizational structure. Where there is such a dispersal of FTI, the agency must centralize safeguarding responsibilities to the greatest extent practical and establish and maintain uniform safeguard standards consistent with IRS guidelines. The official(s) assigned these responsibilities must hold a position high enough in the agency's organizational structure to ensure compliance with the agency safeguard standards and procedures.

The selected official(s), or point(s) of contact (POC(s)) must also be responsible for ensuring that internal inspections are conducted, for submitting required safeguard reports to the IRS, for properly reporting any data breach incidents, and for any necessary liaison with the IRS.

2.6 Safeguard Reviews

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

This includes all FTI received whether from the IRS or a secondary source such as SSA, BFS or another agency (see *Section1.4.1, Federal Tax Information).* Safeguard reviews are conducted to determine the adequacy of safeguards as opposed to evaluating an agency's programs. Several factors will be considered when determining the need for and the frequency of reviews. Reviews are conducted by the IRS Office of Safeguards within the Office of Privacy, Governmental Liaison and Disclosure.

2.7 Conducting the Review

The IRS initiates the review by communication with an agency point of contact (POC). The preliminary discussion will be followed by a formal engagement letter to the agency head, which provides official notification of the planned safeguard review.

This engagement letter outlines what the review will encompass. Additional requests for specific information will be provided to the agency POC. These requests may include a list of records to be reviewed (e.g., training manuals, flowcharts, awareness program documentation, and organizational charts relating to the processing of FTI), the scope and purpose of the review, a list of the specific areas to be reviewed, and agency personnel to be interviewed.

Reviews cover the requirements of IRC 6103(p)(4) which can be found in:

- Section 3.0, *Recordkeeping Requirement*
- Section 4.0, *Secure Storage—IRC 6103(p)(4)(B)*
- Section 5.0, *Restricting Access—IRC 6103(p)(4)(C)*
- Section 6.0, *Other Safeguards—IRC 6103(p)(4)(D)*
- Section 7.0, *Reporting Requirements—6103(p)(4)(E)*
- Section 8.0, *Disposing of FTI—IRC 6103(p)(4)(F)*
- Section 9.0, *Computer System Security*

2.7.1 On-Site Review Process

The on-site review officially begins at the opening conference where procedures and parameters will be communicated. Observing actual operations is a required step in the review process. Sites to be reviewed will be based on the flow of the FTI through the agency, which may include field offices, consolidated data centers, off-site storage facilities, disaster recovery sites, and contractor sites both within and outside the state. Agency files may be spot-checked to determine if they contain FTI. The actual review is followed by a closing conference and issuance of a Preliminary Findings Report (PFR) where the agency is informed of findings identified during the review. A Safeguard Review Report (SRR) and Corrective Action Plan (CAP) will be issued within 45 days of the closing conference to document the on-site review findings. Requests for corrections to the SRR must be emailed to the SafeguardReports@irs.gov mailbox. The Office of Safeguards will respond with acknowledgement and determination.

Table 1 – Safeguard Review Cycle

Action	Notice	Time Frame	Note
Preliminary Discussion	Primary Point of Contact from last review	*120 days ahead of review	*Timeframe is approximate for the preliminary discussion and engagement letter. This may occur closer to the actual review date.
Engagement Letter	Submitted to agency head	*120 to 30 days in advance of review	
Opening Conference	At HQ with agency head, department heads, and IT staff	Day 1 of review 9:00 a.m.	Opening conference will summarize the review.
On-Site Review	Visit to various departments where FTI is located	2 to 3 days	Additional days may be needed as required.

Action	Notice	Time Frame	Note
Closing Conference with Preliminary Findings Report	At HQ with agency head and department heads	Last day of review; will leave PFR for agency	Agency can start working on the findings but must wait until the CAP cycle to report corrective actions. This may be a soft (preliminary) closing if there are additional sites or devices to review.
Final Report	Submitted to agency head	Prepared within 45 days after closing conference	Agency responds with CAP.
CAP Submissions	Report on any corrective action still open from the final report	Submitted semi-annually	Responses must include a status of finding and an actual numerical date of when the planned or actual correction action is taken to address the finding. Subsequent CAP responses are required for all open findings. Evidentiary documentation is required for critical and significant findings.
SSR Submission	Initially report procedures established to protect FTI received from the IRS; reports yearly actions taken to protect FTI and any updates in procedures	Submitted annually	Yearly update to the document will be accompanied by a certification of accuracy by agency head.

2.7.2 Computer Security Review Process

The Office of Safeguards will assess agency compliance with the computer security requirements identified in this publication as part of the on-site review process. Requirements are assessed as they relate to NIST SP 800-53 security controls as outlined in this publication. To ensure a standardized computer security review process, the following techniques will be used to evaluate agency policies, procedures, and IT equipment that receive, process, store, or transmit FTI:

Table 2 – IT Testing Techniques

Automated Compliance and Vulnerability Assessment Testing	Computer Security Reviewers will use a combination of compliance and vulnerability assessment software tools to validate the adequate protection of FTI on agency and contractor owned equipment. These automated tools will be launched from either IRS-issued flash drives or laptop computers. Profiles used with these tools can be downloaded from the Office of Safeguards' website.
SCSEM	Documents and tests hardening requirements for specific technologies used to receive, process, store, or transmit FTI. SCSEMs can and should be downloaded from the Office of Safeguards' website.
MOT	Documents will be requested in advance and expected to be provided prior to the review process, no later than the opening conference.

Agencies should be prepared for the Computer Security Reviewers to use the preceding resources as part of the on-site review. As necessary, agency management approval must be obtained prior to the on-site review, if agency policies and procedure contradict any of these methods.

2.8 Corrective Action Plan

The CAP must be updated and submitted semi-annually on the latest version to the Office of Safeguards (see *Section 7.3, Corrective Action Plan*) until all review findings are accepted and closed by the Office of Safeguards.

The CAP must include a brief explanation of actions already taken or planned to resolve the finding. For all outstanding findings, the agency must detail planned actions and associated milestones for resolution.

All findings must be addressed in a timely fashion. The Office of Safeguards will identify deadlines for resolution based upon the risk associated with each finding. Outstanding issues must be resolved and addressed in the next reporting cycle of the CAP.

2.9 Voluntary Termination of Receipt of FTI

2.9.1 Termination Documentation

When an agency no longer requires FTI, notify Safeguards at SafeguardReports@irs.gov by providing the following:

1. Copies of notifications to all agencies from which FTI is received, that FTI will no longer be requested, and
2. Letter from the Head of Agency certifying that all residual FTI has been destroyed. (See Section 8.0 Disposal of FTI – IRC 6103(p)(4)(F))

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

2.9.2 Archiving FTI Procedure (for agencies terminating receipt of FTI but required by statute to retain FTI for designated periods)

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

- Insure that a currently authorized agency and/or contractor retain FTI in accordance with Publication 1075 security standards
- Provide copies of notifications as shown in 2.9.1 (1. copies of notifications requesting termination of FTI) above
- Submit an annual SSR each year during the retention period
- Continue to be subject to periodic Safeguard Reviews
- Letter from Head of Agency certifying that all residual FTI has been destroyed when the retention period has ended

3.0 Recordkeeping Requirement

3.1 General

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

This recordkeeping must include internal requests among agency employees as well as requests outside of the agency. These records are required to track the movement of FTI. The records are to be maintained for five years or the agency's applicable records control schedule must be followed, whichever is longer. The Safeguards website contains guidance, job aids, helpful tools, and frequently asked questions to assist agencies in meeting safeguard requirements; see http://www.irs.gov/uac/Safeguards-Program.

The agency must establish, maintain, and update at least annually, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing FTI. Provide each update of the FTI inventory to the Chief Information Officer or information security official at least annually to support the establishment of information security requirements for all new or modified information systems containing FTI.

Records must be maintained in accordance with IRS audit log retention requirements for electronic and non-electronic files. For additional guidance, see *Exhibit 9, Record Retention Schedules*.

3.2 Electronic and Non-Electronic FTI Logs

The agency must establish a tracking system to identify and track the location of electronic and non-electronic FTI from receipt until it is destroyed. The FTI log may include tracking elements, such as:

- Taxpayer Name or other identifier*
- Tax year(s)
- Type of information (e.g., revenue agent reports, Form 1040, work papers)
- The reason for the request
- Date requested
- Date received
- Exact location of the FTI
- Who has had access to the data
- If disposed of, the date and method of disposition

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

If the authority to make further disclosures is present (e.g., agents/contractors), information disclosed outside the agency must be recorded on a separate list or log. The log must reflect to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Agencies transmitting FTI from one mainframe computer to another, as in the case of the SSA sending FTI to state human services agencies, need only identify the bulk records transmitted. This identification will contain the approximate number of taxpayer records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.

Figure 1 – Sample FTI Log

Non-Electronic Recordkeeping Log									
Date Requested	Date Received	Taxpayer Name	Tax Year(s)	Type of Information	Reason for Request	Exact Location	Who has access?	Disposition Date	Disposition Method

3.3 Converted Media

Conversion of FTI from paper to electronic media (scanning) or from electronic media to paper (print screens or printed reports) also requires tracking from creation to destruction of the converted FTI. All converted FTI must be tracked on logs containing the fields detailed in Section 3.2, depending upon the current form of the FTI, electronic or non-electronic.

3.4 Recordkeeping of Disclosures to State Auditors

When disclosures are made by a state tax agency to state auditors, recordkeeping requirements pertain only in instances where the auditors use FTI for further scrutiny and inclusion in their work papers. In instances where auditors read large volumes of records containing FTI, whether in paper or electronic format, the state tax agency need only identify bulk records examined. This identification will contain the approximate number of taxpayer records, the date of inspection, a description of the records, and the name of the individual(s) making the inspection. Recordkeeping log samples are provided in Section 3.2.

Disclosure of FTI to state auditors by child support enforcement and human services agencies is not authorized by statute. FTI in case files must be removed prior to access by the auditors

4.0 Secure Storage—IRC 6103(p)(4)(B)

4.1 General

Security may be provided for a document, an item, or an area in a number of ways. These include but are not limited to locked containers of various types, vaults, locked rooms, locked rooms that have reinforced perimeters, locked buildings, guards, electronic security systems, fences, identification systems, and control measures.

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

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

4.2 Minimum Protection Standards

Minimum protection standards (MPS) establish a uniform method of physically protecting data and systems as well as non-electronic forms of FTI. This method contains minimum standards that will be applied on a case-by-case basis. Because local factors may require additional security measures, management must analyze local circumstances to determine location, container, and other physical security needs at individual facilities. MPS have been designed to provide management with a basic framework of minimum security requirements.

The objective of these standards is to prevent unauthorized access to FTI. MPS thus requires two barriers. Example barriers under the concept of MPS are outlined in the following table. Each topic represents one barrier and should be used as a starting point to identify two barriers of MPS to protect FTI.

Table 3 – Minimum Protection Standards

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

The MPS or “two barrier” rule applies to FTI, beginning at the FTI itself and extending outward to individuals without a need-to-know. MPS provides the capability to deter, delay, or detect surreptitious entry. Protected information must be containerized in areas where other than authorized employees may have access after-hours.

Using a common situation as an example, often an agency desires or requires that security personnel or custodial service workers or landlords for non-government-owned facilities have access to locked buildings and rooms. This may be permitted as long as there is a second barrier to prevent access to FTI. A security guard, custodial services worker, or landlord may have access to a locked building or a locked room if FTI is in a locked security container. If FTI is in a locked room but not in a locked security container, the guard, janitor, or landlord may have a key to the building but not the room.

Additional controls have been integrated into this document that map to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4. These are identified in *Section 9.3, NIST SP 800-53 Control Requirements.* Per NIST guidelines, policies and procedures must be developed, documented, and disseminated, as necessary, to facilitate implementing physical and environmental protection controls.

For additional guidance, see *Section 9.3.11.3, Physical Access Control (PE-3)*.

4.3 Restricted Area Access

Care must be taken to deny unauthorized access to areas containing FTI during duty and non-duty hours. This can be accomplished by creating restricted areas, security rooms, or locked rooms. Additionally, FTI in any form (computer printout, photocopies, tapes, notes) must be protected during non-duty hours. This can be done through a combination of methods, including secured or locked perimeter, secured area, or containerization.

A restricted area is an area where entry is limited to authorized personnel (individuals assigned to the area). All restricted areas either must meet secured area criteria or provisions must be made to store FTI in appropriate containers during non-duty hours. Using restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized access or disclosure or theft of FTI. All of the following procedures must be implemented to qualify as a restricted area.

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

A restricted area visitor log must be maintained at a designated entrance to the restricted area, and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance.

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

- Name and organization of the visitor
- Signature of the visitor
- Form of identification
- Date of access
- Time of entry and departure
- Purpose of visit
- Name and organization of person visited

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

Each restricted area access log must be closed out at the end of each month and reviewed by management.

Figure 2 – Sample Visitor Access Log

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

For additional guidance on visitor access requirements, see *Section 9.3.11.7, Visitor Access Records (PE-8)*.

4.3.1 Use of Authorized Access List

To facilitate the entry of employees who have a frequent and continuing need to enter a restricted area, but who are not assigned to the area, an Authorized Access List (AAL) can be maintained so long as MPS are enforced *(see Section 4.2, Minimum Protection Standards).*

Agency Employees: The AAL must contain the following:

- Name of individual
- Agency or department name
- Name and phone number of agency POC
- Address of agency POC
- Purpose for access

The AAL for agency employees must be updated at least annually or when employee access changes.

Vendors and Non-Agency Personnel: The AAL must contain the following information:

- Name of vendor/contractor/non-agency personnel
- Name and phone number of agency Point of Contact authorizing access
- Name and address of vendor POC
- Address of vendor/contractor
- Purpose and level of access

Vendors, contractors, and non-agency personnel AAL must be updated monthly.

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

For additional guidance, see *Section 9.3.11.2, Physical Access Authorizations (PE-2).* Also, see *Section 9.3.11.8, Delivery and Removal (PE-16)*, for guidance on controlling information system components entering and exiting the restricted area.

4.3.2 Controlling Access to Areas Containing FTI

Management or a designee shall maintain an authorized list of all personnel who have access to information system areas, where these systems contain FTI. This shall not apply to those areas within the facility officially designated as publicly accessible.

The agency shall issue appropriate authorization credentials, including badges, identification cards, or smart cards. In addition, a list shall be maintained that identifies those individuals who have authorized access to any systems where FTI is housed. Access authorizations and records maintained in electronic form are acceptable.

Each agency shall control physical access to the information system devices that display FTI information or where FTI is processed to prevent unauthorized individuals from observing the display output. For additional information, see *Section 9.3.11.5, Access Control for Output Devices (PE-5)*.

The agency or designee shall monitor physical access to the information system where FTI is stored to detect and respond to physical security incidents. For additional information, see *Section 9.3.11.6, Monitoring Physical Access (PE-6)*.

For all areas that process FTI, the agency shall position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. For additional guidance, see *Section 9.3.11.10, Location of Information System Components (PE-18)*.

Whenever cleaning and maintenance personnel are working in restricted areas containing FTI, the cleaning and maintenance activities must be performed in the presence of an authorized employee.

Allowing an individual to “piggyback” or “tailgate” into restricted locations must be prohibited and documented in agency policy. The agency must ensure that all individuals entering an area containing FTI do not bypass access controls or allow unauthorized entry of other individuals. Unauthorized access must be challenged by authorized individuals (e.g., those with access to FTI). Security personnel must be notified of piggyback/tailgate attempts.

4.3.3 Control and Safeguarding Keys and Combinations

All containers, rooms, buildings, and facilities containing FTI must be locked when not in actual use.

Access to a locked area, room, or container can be controlled only if the key or combination is controlled. Compromising a combination or losing a key negates the security provided by that lock. Combinations to locks must be changed annually or when an employee who knows the combination retires, terminates employment or transfers to another position.

Combinations must be given only to those who have a need to have access to the area, room, or container and must never be written on a sticky-note, calendar pad, or any other item (even though it is carried on one's person or hidden from view). An envelope containing the combination must be secured in a container with the same or a higher security classification as the highest classification of the material authorized for storage in the container or area the lock secures.

Keys must be issued only to individuals having a need to access an area, room, or container. Inventory records must be maintained on keys and must account for the total keys available and keys issued. The inventory must account for master keys and key duplicates. A annual reconciliation must be done on all key records. The number of keys or persons with knowledge of the combination to a secured area will be kept to a minimum. Keys and combinations will be given only to those individuals who have a frequent need to access the area.

4.3.4 Locking Systems for Secured Areas

The number of keys or persons with knowledge of the combination to a secured area will be kept to a minimum. Keys and combinations will be given only to those individuals who have a frequent need to access the area.

Access control systems (e.g., badge readers, smart cards, and biometrics) that provide the capability to audit access control attempts must maintain audit records with successful and failed access attempts to secure areas containing FTI or systems that process FTI. Agency personnel must review access control logs on a monthly basis. The access control log must contain the following elements:

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

4.4 FTI in Transit

Handling FTI must be such that the FTI does not become misplaced or available to unauthorized personnel.

Any time FTI is transported from one location to another, care must be taken to provide appropriate safeguards. When FTI is hand-carried by an individual in connection with a trip or in the course of daily activities, it must be kept with that individual and protected from unauthorized disclosures.

All shipments of paper or electronic FTI (including compact disk [CD], digital video disk [DVD], thumb drives, hard drives, tapes, and microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service must be double-sealed; that is, one envelope within another envelope. The inner envelope must be marked "confidential" with some indication that only the designated official or delegate is authorized to open it. The outermost envelope should not be labelled as FTI or provide any indication that the contents contains FTI, since that may actually increase risk to the contents. Using sealed boxes serves the same purpose as double-sealing and prevents anyone from viewing the contents thereof.

4.5 Physical Security of Computers, Electronic, and Removable Media

Computers and electronic media that receive, process, store, or transmit FTI must be in a secure area with restricted access. In situations when requirements of a secure area with restricted access cannot be maintained, such as home work sites, remote terminals or other office work sites, the equipment must receive the highest level of protection practical, including full disk encryption. All computers and mobile devices that contain FTI and reside at an alternate work site must employ encryption mechanisms to ensure that FTI may not be accessed if the computer is lost or stolen (see OMB M-06-16).

Basic security requirements must be met, such as keeping FTI locked up when not in use. When removable media contains FTI, it must be labeled as FTI.

All computers, electronic media, and removable media containing FTI, must be kept in a secured area under the immediate protection and control of an authorized employee or locked up. When not in use, the media must be promptly returned to a proper storage area/container.

Inventory records of electronic media must be maintained and reviewed semi-annually for control and accountability. *Section 3.0, Recordkeeping Requirement*, contains additional information. For additional guidance on log retention requirements, see *Exhibit 9, Record Retention Schedules*.

For physical security protections of transmission medium (e.g., cabling), see *Section 9.3.11.4, Access Control for Transmission Medium (PE-4)*.

4.6 Media Off-Site Storage Requirements

Media containing FTI which is sent to an off-site storage facility, must be properly secured, labelled, and protected from access by unauthorized individuals at all times. The media may not be stored on open shelving, unless the shelving is in a restricted area (see Restricted Area Access, Section 4.3) accessible only to individuals with authorized access to FTI. The agency must ensure that contractor-operated off-site storage facilities maintaining FTI on open shelving comply with all safeguarding requirements (e.g., visitor access logs, internal inspections, contractor access restrictions, employee training, and the contract include Exhibit 7 safeguarding language). These facilities are subject to IRS safeguard reviews.

Agencies which do not have the statutory authority to contract for services that involve the disclosure of FTI (e.g. state Child Support Enforcement, Human Services and certain workforce agencies (not receiving data under 6103(d)), may not allow release media containing FTI to a contractor operated off-site storage facility unless the following conditions are met:

- The media is encrypted and labelled as containing “federal tax information”
- The media is locked in a turtle case or security container
- The agency retains the key to the turtle case

4.7 Telework Locations

If the confidentiality of FTI can be adequately protected, telework sites, such as employee’s homes or other non-traditional work sites can be used. FTI remains subject to the same safeguard requirements and the highest level of attainable security. All of the requirements of *Section 4.5, Physical Security of Computers, Electronic, and Removable Media*, apply to telework locations.

The agency must conduct periodic inspections of alternative work sites during the year to ensure that safeguards are adequate. The results of each inspection shall be fully documented. IRS reserves the right to visit alternative work sites while conducting safeguard reviews. Changes in safeguard procedures must be described in detail by the agency in the SSR. For additional information, see *Section 7.2, Safeguard Security Report*.

4.7.1 Equipment

The agency must retain ownership and control, for all hardware, software, and end-point equipment connecting to public communication networks, where these are resident at all alternate work sites. The use of virtual desktop infrastructure with non-agency-owned devices (including personally-owned devices) is an acceptable alternative, where all requirements in section *9.4.13 Virtual Desktop Infrastructure* are met.

Employees must have a specific room or area in a room that has the appropriate space and facilities for the type of work done. Employees also must have a way to communicate with their managers or other members of the agency if security problems arise.

The agency must give employees locking file cabinets or desk drawers so that documents, disks, and tax returns may be properly secured when not in use. If agency furniture is not furnished to the employee, the agency must ensure that an adequate means of storage exists at the work site. The agency must provide “locking hardware” to secure automated data processing equipment to large objects, such as desks or tables. Smaller, agency-owned equipment must be locked in a filing cabinet or desk drawer when not in use.

4.7.2 Storing Data

FTI may be stored on hard disks only if agency-approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance including upgrades, and are being used. Access controls must include password security, an audit trail, encryption, virus detection, and data overwriting capabilities.

4.7.3 Other Safeguards

Only agency-approved security access control devices and agency-approved software will be used. Copies of illegal and non-approved software will not be used. Electronic media that is to be reused must have files overwritten or degaussed.

The agency must maintain a policy for the security of alternative work sites. The agency must coordinate with the managing host system(s) and any networks and maintain documentation on the test. Before implementation, the agency will certify that the security controls are adequate for security needs. Additionally, the agency will promulgate rules and procedures to ensure that employees do not leave computers unprotected at any time. These rules must address brief absences while employees are away from the computer. The agency must provide specialized training in security, disclosure awareness, and ethics for all participating employees and managers. This training must cover situations that could occur as the result of an interruption of work by family, friends, or other sources.

5.0 Restricting Access—IRC 6103(p)(4)(C)

5.1 General

Agencies are required by IRC 6103(p)(4)(C) to restrict access to FTI only to persons whose duties or responsibilities require access (see *Exhibit 2, USC Title 26, IRC 6103(p)(4)*, and *Exhibit 4, Sanctions for Unauthorized Disclosure*). To assist with this requirement, FTI must be clearly labeled "Federal Tax Information" and handled in such a manner that it does not become misplaced or available to unauthorized personnel. Additionally, warning banners advising of safeguarding requirements must be used for computer screens (see *Exhibit 8, Warning Banner Examples)*.

To understand the key terms of *unauthorized disclosure*, *unauthorized access*, and *need-to-know*, see *Section 1.4, Key Definitions*.

5.1.1 Background Investigation Minimum Requirements

Determining the suitability of individuals who require access to U.S. government Sensitive But Unclassified (SBU) information, including FTI, is a key factor in ensuring adequate information security. Prior to granting access to FTI, and periodically thereafter, the Agency must complete a suitability background investigation which is favorably adjudicated by the Agency.

Federal agencies must conduct a suitability or security background investigation based on the position sensitivity of the individual's assigned position and risk designation associated with the investigative Tier established by the Federal Investigative Standards (FIS). Granting access to FTI requires a Tier 2 level investigation at a minimum.

A FIS Tier 2 standard background investigation meets the suitability investigative requirement for non-sensitive positions designated as moderate risk public trust (requested using Standard Form 85P). Investigations conducted at Tiers 2-5 meet the minimum standard for an employee or contractor access to FTI. Federal agencies may be asked to provide evidence that the required BI was conducted for each individual granted access to FTI. FIS standards require reinvestigation every five years at a minimum.

State and local agencies which are not required to implement the federal background investigation standards must establish a personnel security program that ensures a background investigation is completed at the appropriate level for any individual who will have access to FTI using the guidance below as the minimum standard and a reinvestigation conducted within 10 years at a minimum.

- Agencies must develop a written policy requiring that employees, contractors and sub-contractors (if authorized), with access to FTI must complete a background investigation that is favorably adjudicated. The policy will identify the process, steps,

timeframes and favorability standards that the agency has adopted. The agency may adopt the favorability standards set by the FIS or one that is currently used by another state agency, or the Agency may develop its own standards specific to FTI access.

- The written background investigation policy must establish a result criterion for each required element which defines what would result in preventing or removing an employee's or contractor's access to FTI.

- Agencies must initiate a background investigation for all employees and contractors prior to permitting access to FTI.

- State agencies must ensure a reinvestigation is conducted within 10 years from the date of the previous background investigation for each employee and contractor requiring access to FTI.

- Agencies must make written background investigation policies and procedures as well as a sample of completed employee and contractor background investigations available for inspection upon request.

- Background investigations for any individual granted access to FTI must include, at a minimum:

    a) FBI fingerprinting (FD-258) - review of Federal Bureau of Investigation (FBI) fingerprint results conducted to identify possible suitability issues. (Contact the appropriate state identification bureau for the correct procedures to follow.) A listing of state identification bureaus can be found at: https://www.fbi.gov/about-us/cjis/identity-history-summary-checks/state-identification-bureau-listing

    This national agency check is the key to evaluating the history of a prospective candidate for access to FTI. It allows the Agency to check the applicant's criminal history in all 50 states, not only current or known past residences.

    b) Check of 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.

    The local law enforcement check will assist agencies in identifying trends of misbehavior that may not rise to the criteria for reporting to the FBI database but is a good source of information regarding an applicant.

    c) Citizenship/residency – 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).

Employers must complete USCIS Form I-9 to document verification of the identity and employment authorization of each new employee hired after November 16, 1986, to work in the United States. Within 3 days of completion, any new employee must also be processed through E-Verify to assist with verification of his/her status and the documents provided with the Form I-9. The E-Verify system is free of charge and can be located at www.uscis.gov/e-verify. This verification process may only be completed on new employees. Any employee with expiring employment eligibility must be documented and monitored for continued compliance.

5.1.2 Implementing the Background Investigation Requirement

The requirements of Section 5.1.1 pertaining to initial and periodic background investigations for individuals before authorizing access to FTI is effective upon date of this publication. Implementation of the new standards, including the development of written policies and verification that all individuals with access to FTI have an appropriate level of investigation and initiating new required investigations to comply with the requirement may occur within one year.

Upon publication, agencies should initiate action to establish a written background investigation policy that conforms to the standards of Section 5.1.1. Agencies should also identify all employees or contractors who currently have access to FTI and have not completed the required personnel security screening and initiate a background investigation which meets these standards. Agencies should initiate a background investigation for all newly hired employees and contractors who will require access to FTI to perform assigned duties as soon as practicable upon notification of the requirement.

Federal agencies that completed a Moderate-Risk Background Investigation (MBI) or higher, for individuals with access to FTI, prior to the October 2014 implementation date of the FIS Tier 2 standard investigation, have met the minimum standard and no further investigation is needed so long as reinvestigation is timely scheduled. Individuals granted access to FTI based on a National Agency Check with Inquiries (NACI) is not sufficient and a Tier 2 investigation should be initiated for continued access to FTI.

Agency implementation efforts to achieve full compliance with the minimum background investigation requirement may vary based on based on state legislation, budget and labor relation hurdles. Some state agencies have published standards which meet or exceed these requirements while others may have minimal or no standards established for background investigations. The expectation is that all agencies receiving FTI will take the steps necessary towards full compliance with this requirement.

As a part of the annual Safeguard Security Report, (SSR), and during an agency on-site review, compliance with and efforts underway to achieve compliance will be evaluated. Any deficiencies will be documented in the agency's Corrective Action Plan, (CAP), and there will be an expectation that each agency response includes an update on progress and a plan to continue moving forward towards compliance.

5.2 Commingling of FTI

Commingling of FTI refers to having FTI and non-FTI data stored together, regardless of format. For example, commingling occurs when FTI is included in sentence of text in a paper notice or letter; a row or column containing FTI a database table; files stored on electronic media (some files containing FTI and some don't),or at a shared data center with some systems including FTI subject to access restrictions (and some don't). Any kind of commingling creates the need for additional controls, since the introduction of FTI requires the entire letter, data table, removable media, etc to be handled and protected as FTI.

It is recommended that FTI be kept physically and logically separate from other information to the maximum extent possible to avoid inadvertent disclosures and need for additional controls. Agencies should attempt to avoid maintaining FTI as part of their case files including any recordation or transcription in case notes or activity logs, whether paper or electronic.
In situations where physical separation is impractical, the file must be clearly labeled to indicate that FTI is included, and the file must be safeguarded.

All FTI must be removed prior to releasing files to an individual or agency without authorized access to FTI.

5.2.1 Commingling of Electronic Media

If FTI is recorded on electronic media (e.g., tapes) with other data, it must be protected as if it were entirely FTI. Such commingling of data on electronic media should be avoided, if practicable. FTI only loses its character when it is verified by a third party and overwritten in the agency's records.

When data processing equipment is used to process or store FTI and the information is mixed with agency data, access must be controlled by:

- Restricting computer access only to authorized personnel
- Systemic means, including labeling; for additional information, see *Section 9.3.10.3, Media Marking (MP-3)*
- When technically possible, data files, data sets, and shares must be overwritten after each use

Commingled data at multi-purpose facilities results in security risks that must be addressed. If the agency shares physical or computer facilities with other agencies, departments, or individuals not authorized to have FTI, strict controls—physical and systemic—must be maintained to prevent unauthorized disclosure of this information.

Examples of commingling include:

- If the document has both FTI and information provided by the individual or third party, commingling has occurred, and the document must also be labeled and safeguarded. If the individual or a third party from its own source provides the information, this is not FTI. *Provided* means actually giving the information on a separate document, not just verifying and returning a document that includes FTI.

- If a new address is received from IRS records and entered into a computer database, the address must be identified as FTI and safeguarded. If the individual or third party subsequently provides the address independently, the address will not be considered FTI as long as the address is overwritten by replacing the IRS source address with the newly provided information, non-IRS source address. Again, *provided* means using individual or third-party knowledge or records as the source of information, which does not include FTI.

5.3 Access to FTI via State Tax Files or Through Other Agencies

Some state disclosure statutes and administrative procedures permit access to state tax files by other agencies, organizations, or employees not involved in tax matters. As a general rule, IRC 6103(d) does not permit access to FTI by such employees, agencies, or other organizations. The IRC clearly provides that FTI will be furnished to state tax agencies only for tax administration purposes and made available only to designated state tax personnel and legal representatives or to the state audit agency for an audit of the tax agency. Questions about whether particular state employees are entitled to access FTI must be forwarded to the Disclosure Manager at the IRS Office that serves your location.[†] Generally, the IRC does not permit state tax agencies to furnish FTI to other state agencies or to political subdivisions, such as cities or counties. State tax agencies may not furnish FTI to any other state or local agency, even where agreements have been made, informally or formally, for the reciprocal exchange of state tax information unless formally approved by the IRS. Also, non-government organizations, such as universities or public interest organizations performing research cannot have access to FTI.

Although state tax agencies are specifically addressed previously in this section, the restrictions on data access and non-disclosure to another agency or third party applies to all agencies authorized to receive FTI. Generally, statutes that authorize disclosure of FTI do not authorize further disclosures by the recipient agency. Unless IRC 6103 provides for further disclosures by the agency, the agency cannot make such disclosures or otherwise grant access to FTI to either employees of another component of the agency not involved with administering the program for which the FTI was specifically received or to another state agency for any purpose.

Agencies and subdivisions within an agency may be authorized to obtain the same FTI for different purposes, such as a state tax agency administering tax programs and a component human services agency administering benefit eligibility verification programs (IRC 6103(l)(7)) or child support enforcement programs (IRC 6103(l)(6)).

[†] Refer to http://www.irs.gov/uac/IRS-Disclosure-Offices for contact information.

However, the IRC disclosure authority does not permit agencies or subdivisions of agencies to exchange or make subsequent disclosures of this information for another authorized purpose even within the agency. In addition, unless specifically authorized by the IRC, agencies are not permitted to allow access to FTI to agents, representatives, or contractors.

FTI cannot be accessed by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies or military installations. Further, FTI may not be received, processed, stored, transmitted, or disposed of by information technology (IT) systems located offshore.

5.4 Controls over Processing

The agency must establish adequate controls to prevent disclosing FTI to other state agencies, tax or non-tax, or to political subdivisions, such as cities or counties, for any purpose, including tax administration, absent explicit written IRS authority granted under IRC 6103(p)(2)(B).

Processing of FTI in an electronic media format including removable media, microfilms, photo impressions, or the conversion to other formats (including tape reformatting or duplication, reproduction or conversion to digital images or hard copy printout) will be performed as indicated in the following environments.

5.4.1 Agency Owned and Operated Facility

Processing under this method will take place in a manner that will protect the confidentiality of the information on the electronic media. All safeguards outlined in this publication also must be followed and will be subject to IRS safeguard reviews.

5.4.2 Contractor or Agency Shared Facility - Consolidated Data Centers

5.4.2.1 Agency Shared Facilities:

Recipients of FTI are allowed to use a shared facility but only in a manner that does not allow access to FTI by employees, agents, representatives, or contractors of other agencies using the shared facility.

> *For purposes of applying sections 6103(l), (m), and (n), the term* agent *includes contractors.*

Access restrictions pursuant to the IRC authority by which the FTI is received continue to apply; for example, human services agencies administering benefit eligibility programs may not allow contractors, including consolidated data center contractors, access to any FTI.

The agency must include, as appropriate, the requirements specified in *Exhibit 7, Safeguarding Contract Language*, in accordance with IRC 6103(n).

In addition to the agency being subject to Safeguard reviews, all contractor and shared sites that receive, process, store or transmit FTI are subject to reviews.

> *These requirements also apply to releasing electronic media to a private contractor or other agency office, even if the purpose is merely to erase the old media for reuse.*

***5.4.2.2 Consolidated Data Centers*:**

Agencies using consolidated data centers must implement appropriate controls to ensure the protection of FTI, including a service level agreement (SLA) between the agency authorized to receive FTI and the consolidated data center. The SLA must cover the following:

- The agency with authority to receive FTI is responsible for ensuring the protection of all FTI received. The consolidated data center shares responsibility for safeguarding FTI.
- The SLA provides written notification to the consolidated data center management that they are bound by the provisions of Publication 1075, relative to protecting all FTI within their possession or control.
- The SLA shall detail the IRS' right to inspect consolidated data center facilities and operations accessing, receiving, storing or processing FTI under this agreement to assess compliance with requirements defined in IRS Publication 1075. The SLA shall specify that IRS' right of inspection includes the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI.
- The SLA shall detail the consolidated data center's responsibilities to address corrective action recommendations to resolve findings of noncompliance identified by IRS inspections.
- The agency will conduct an internal inspection of the consolidated data center every 18 months, as described in Section 6.4, *Internal Inspections*. Multiple agencies sharing a consolidated data center may partner together to conduct a single, comprehensive internal inspection. However, care must be taken to ensure agency representatives do not gain unauthorized access to other agencies' FTI during the internal inspection.

- The employees from the consolidated data center with access to or use of FTI, including system administrators and programmers, must:
    1) meet the background check requirements defined in IRS Publication1075 and
    2) prior to initial access to or use of FTI, as well as annually thereafter, receive disclosure awareness training and sign a confidentiality statement. These provisions also extend to any contractors hired by the consolidated data center that have authorized access to or use of FTI.
- The specific data breach incident reporting procedures for all consolidated data center employees and contractors must be covered. The required disclosure awareness training must include a review of these procedures.
- The Exhibit 7 language must be included in the contract between the recipient agency and the consolidated data center, including all contracts involving contractors hired by the consolidated data center.
- Responsibilities must be identified for coordination of the 45-day notification of the use of contractors or subcontractors with access to FTI.

Generally, consolidated data centers are either operated by a separate state agency (e.g., Department of Information Services) or by a private contractor. If an agency is considering transitioning to either a state-owned or private vendor consolidated data center, the Office of Safeguards strongly suggests the agency submit a request for discussions with Safeguards as early as possible in the decision making or implementation planning process. The purpose of these discussions is to ensure the agency remains compliant with safeguarding requirements during the transition to the consolidated data center.

5.4.3 Review Availability of Contractor Facilities:

As ~~a~~ part of the agency review process, all affiliated contractors who receive, transmit, process and store FTI on behalf of the agency are subject to review and testing.

The agency must include Exhibit 7, Safeguarding Contract Language, in accordance with IRC 6103(n) for all contracts. Agencies seeking to modify this language must secure approval from Safeguards in advance.

These requirements also apply to releasing electronic media to a private contractor or other agency office, even if the purpose is merely to erase the old media for reuse.

5.5 Child Support Agencies—IRC 6103(l)(6), (l)(8), and (l)(10)

In general, no officer or employee of any state or local child support enforcement agency can make further disclosures of FTI.

However, limited information may be disclosed to agents or contractors of the agency for the purpose of, and to the extent necessary in, establishing and collecting child support obligations from and locating individuals owing such obligations.

The information that may be disclosed for this purpose to an agent or a contractor is limited to:

- The address;
- Social Security Number of an individual with respect to whom child support obligations are sought to be established or enforced; and/or
- The amount of any reduction under IRC 6402(c) in any overpayment otherwise payable to such individual.

Tax refund offset payment information may not be disclosed by any federal, state, or local child support enforcement agency employee, representative, agent, or contractor into any court proceeding. To satisfy the re-disclosure prohibition, submit only payment date and payment amount for all payment sources (not just tax refund offset payments) into court proceedings.

> *Forms 1099 and W-2 information are not authorized by statute to be disclosed to contractors under the child support enforcement program (IRC 6103(l)(6).*

5.6 Human Services Agencies—IRC 6103(l)(7)

No officer or employee of any federal, state, or local agency administering certain programs under the Social Security Act, the Food Stamp Act of 1977, or Title 38, United States Code, or certain housing assistance programs is permitted to make further disclosures of FTI for any purpose. Human services agencies may not contract for services that involve the disclosure of FTI to contractors.

5.7 Deficit Reduction Agencies—IRC 6103(l)(10)

Agencies receiving FTI from the Bureau of Fiscal Service related to tax refund offsets are prohibited from making further disclosures of the FTI received unless authorized.

5.8 Centers for Medicare and Medicaid Services—IRC 6103(l)(12)(C)

The Administrator of the Centers for Medicare and Medicaid Services (CMS) is authorized under IRC 6103(l)(12)(C) to disclose FTI it receives from SSA to its agents for the purpose of, and to the extent necessary in, determining the extent that any Medicare beneficiary is covered under any group health plan. A contractual relationship must exist between CMS and the agent. The agent, however, is not authorized to make further disclosures of FTI for any purpose.

5.9 Disclosures under IRC 6103(l)(20)

Disclosures to officers, employees, and contractors of SSA and other specified agencies are authorized to receive specific tax information for the purpose of carrying out the Medicare Part B premium subsidy adjustment and Part D Base Beneficiary Premium Increase. These disclosures are subject to safeguard requirements. Any agency receiving FTI from SSA authorized by this provision is also subject to IRS safeguard requirements and review.

5.10 Disclosures under IRC 6103(l)(21)

Disclosures to officers, employees, and contractors of the U.S. Department of Health and Human Services (HHS) at the request of a taxpayer seeking financial assistance for health insurance affordability programs. HHS may release FTI to an Exchange established under the Affordable Care Act or a state agency administering eligibility determinations for Medicaid or Children's Health Insurance Programs for the purpose of establishing eligibility for participation in the Exchange, verifying the appropriate amount of any credits, and determining eligibility for participation in the state program. These disclosures are subject to safeguard requirements. Any agent or contractor is also subject to IRS safeguard requirements and review. IRC 6103(l)(21)(C) may allow the Office of Inspector General, HHS to have access to FTI maintained in the eligibility records of an Exchange or state entity administering these programs, under certain limited circumstances. This authority does not extend to independent state audit agencies which may not have access to FTI in eligibility records unless a contractual relationship is established which conforms to the disclosure requirements of IRC 6103.

5.11 Disclosures under IRC 6103(i)

Federal law enforcement agencies receiving FTI pursuant to court orders or by specific request under Section 6103(i) for purposes of investigation and prosecution of non-tax federal crimes, or to apprise of or investigate terrorist incidents, are subject to safeguard requirements and review.

The Department of Justice must report in its SSR the number of FTI records provided and to which federal law enforcement agency the data was shared for the calendar year processing period.

5.12 Disclosures under IRC 6103(m)(2)

Disclosures to agents of a federal agency under IRC 6103(m)(2) are authorized for the purposes of locating individuals in collecting or compromising a federal claim against the taxpayer in accordance with Sections 3711, 3717, and 3718 of Title 31. If the FTI is shared with agents or contractors, the agency and agent or contractor are all subject to IRS safeguarding requirements and reviews.

6.0 Other Safeguards—IRC 6103(p)(4)(D)

6.1 General

IRC 6103(p)(4)(D) requires that agencies receiving FTI to provide other safeguard measures, as appropriate, to ensure the confidentiality of the FTI. Agencies are required to provide a training program for their employees and contractors.

6.2 Training Requirements

Education and awareness are necessary to provide employees, contractors, and other persons with the information to protect FTI. There are multiple components to a successful training program. In this section, training requirements are consolidated to ensure agencies understand all of the requirements to comply with this publication.

Disclosure awareness training is described in detail within *Section 6.3, Disclosure Awareness Training*. Additional training requirements are located in various sections of the document and identified in the following table.

Table 4 – Training Requirements

Training Component	Applicability	Section
Disclosure Awareness Training	• Unique to protection of FTI and prevention of unauthorized disclosure	6.3
Security Awareness Training	• Provides basic security awareness training to information system users	9.3.2.2
Role-Based Training	• Provides individualized training to personnel based on assigned security roles and responsibilities	9.3.2.3
Contingency Training	• Provides individualized training to personnel based on assigned roles and responsibilities as they relate to recovery of backup copies of FTI	9.3.6.3
Incident Response Training	• Provides individuals with agency-specific procedures to handle incidents • Provides individuals with IRS-specific requirements pertaining to incidents involving FTI	9.3.8.2 and 10.0

6.3 Disclosure Awareness Training

Employees and contractors must maintain their authorization to access FTI through annual training and recertification. Prior to granting an agency employee or contractor access to FTI, each employee or contractor must certify his or her understanding of the agency's security policy and procedures for safeguarding IRS information.

Disclosure awareness training stipulates that:

- Employees and contractors must be advised of the penalty provisions of IRC-Sections 7431, 7213, and 7213A (see *Exhibit 4, Sanctions for Unauthorized Disclosure*, and *Exhibit 5, Civil Damages for Unauthorized Disclosure*).
- The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches (see *Section 10.0, Reporting Improper Inspections or Disclosures*).
- During this training, agencies must make employees aware that disclosure restrictions and penalties apply even after employment with the agency has ended.
- For the initial certification and the annual recertification, the employee or contractor must sign, either with ink or electronic signature, a confidentiality statement certifying his or her understanding of penalty provisions and the security requirements. It must also contain a statement that the employee understands they must report possible improper inspection or disclosure of FTI, including breaches and security incidents to both TIGTA and Safeguards.

  Example: I understand the penalty provisions of IRC 7431, 7213 and 7213A.
  Example: I understand upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, I must follow the proper incident reporting requirements to ensure the Office of Safeguards and the Treasury Inspector General for Tax Administration are notified of a possible issue involving FTI.

- The initial certification and recertification must be documented and placed in the agency's files for review and retained for at least five years.

Additional security and information requirements can be expressed to appropriate personnel by using a variety of methods, such as, but not limited to:

- Additional formal and informal training
- Discussion at group and managerial meetings
- Security bulletin boards throughout the secure work areas
- Security articles in employee newsletters
- Pertinent articles that appear in the technical or popular press to share with members of the management staff
- Posters to display with short simple educational messages (e.g., instructions on reporting unauthorized access "UNAX" violations, address), and
- Email and other electronic messages to inform users

6.3.1 Disclosure Awareness Training Products

The following resources are available from the IRS to assist your agency in meeting the federal safeguard requirements for disclosure awareness and the protection of FTI. Technical information is available to you on the Office of Safeguards website at https://www.irs.gov/uac/safeguards-program.

Some of the following products can be ordered from the IRS Distribution Center by calling 800-TAX-FORM (829-3676). Be sure to identify yourself as a (state) government employee, provide the publication number and quantity. All products will be delivered to the agency address you provide and to the attention of the person you specify. Please do not call the tax help number (800-829-4933). If you experience an ordering problem send an email to SafeguardReports@irs.gov mailbox.

Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies (Key publication explains the federal safeguard requirements)

- Only available online: http://www.irs.gov/pub/irs-pdf/p1075.pdf

Safeguards Disclosure Awareness Videos (Explains key safeguard concepts for protecting the confidentiality of FTI)

- Available online through Safeguards website: https://www.irs.gov/uac/irs-disclosure-awareness-videos
- For DVD availability, please send an email to SafeguardReports@irs.gov

Protecting FTI, Pocket Guide for Government Employees (Provides basic disclosure concepts and warns of civil and criminal sanctions for misuse of FTI)

- Available through Distribution Center: Publication 4761 (Rev. 09-2013)

UNAX Don't Go There!

- Available through Distribution Center:: Bold beige, orange and blue print raises awareness that unauthorized access is UNAX - Poster 11"x17" poster— Document 12800 (Rev. 03-2013)
- Available through Distribution Center: Tri-fold handout—Document 12612 (Rev. 05-2012)

Disclosure Awareness Video—Protecting FTI: A Message from the IRS (Discusses what access to FTI is, how to safeguard it, and how disclosures of that information are protected by federal law)

- Available online through Safeguards website: https://www.irs.gov/uac/irs-disclosure-awareness-videos

6.4 Internal Inspections

Another measure IRS requires is internal inspections by the recipient agency. The purpose is to ensure that the security policies and procedures established by the agency to protect FTI are functioning, maintained and enforced. The agency must submit copies of these inspections to the IRS with the SSR (see *Section 7.2, Safeguard Security Report*). To provide an objective assessment, the inspection must be conducted by a function other than the using function.

To provide reasonable assurance that FTI is adequately safeguarded, the inspection must address the safeguard requirements the IRC and the IRS impose. The agency monitors and audits privacy controls and internal privacy policy to ensure effective implementation.

Agencies must establish a review cycle as follows:

- Local offices receiving FTI: at least every three years
- Headquarters office facilities housing FTI and the agency computer facility: at least every 18 months
- All contractors with access to FTI, including a consolidated data center or off-site storage facility: at least every 18 months

The agency must complete a documented schedule (internal inspection plan), detailing the timing of all internal inspections in the current year and next two years (three-year cycle). The plan must be included as part of the SSR, as described in Section 7.2.

Inspection reports, including a record of corrective actions, must be retained by the agency for a minimum of five years from the date the inspection was completed. IRS personnel may review these reports during an on-site safeguard review. A summary of the agency's findings and the actions taken to correct any deficiencies must be included with the SSR submitted to the IRS.

Key areas that must be addressed include recordkeeping, secure storage, limited access, disposal, and computer security.

6.4.1 Recordkeeping

Each agency and function within that agency shall maintain a log of all requests for FTI, including receipt and disposal of returns or return information. This includes any medium containing FTI, such as computer tapes, cartridges, CDs, or data received electronically.

6.4.2 Secure Storage

FTI (including tapes, cartridges, or other removable media) must be stored in a secure location, safe from unauthorized access.

6.4.3 Limited Access

Access to returns and return information (including tapes, cartridges, or other removable media) must be limited to only those employees, officers, and contractors who are authorized access by law or regulation and whose official duties require such access.

The physical and systemic barriers to unauthorized access must be reviewed and reported. An assessment of facility security features must be included in the report.

6.4.4 Disposal

Upon completion of use, agencies must ensure that the FTI is destroyed or returned to the IRS or the SSA according to the guidelines contained in *Section 8.0, Disposing of FTI—IRC 6103(p)(4)(F).*

6.4.5 Computer Systems Security

The agency's review of the adequacy of its computer security provisions must provide reasonable assurance that access to FTI is limited to personnel who have a need- to-know. This need-to-know must be enforced electronically as well as physically (see Internal Inspection Template on the Office of Safeguards website and *Section 9.3.1, Access Control*, and other portions of Section 9.0, Computer System Security, as applicable).

> *The review of the computer facility must include the evaluation of computer security and physical security controls.*

6.5 Plan of Action and Milestones

The agency must implement a process for ensuring that a Plan of Action and Milestones (POA&M) is developed and monitored. The POA&M must include the corrective actions identified during the internal inspections and will identify the actions the agency plans to take to resolve these findings.

> *The POA&M pertains to findings identified by the agency during the internal inspections process and any other internal or external audit.*
>
> *The CAP covers findings identified by the Office of Safeguards during the on-site safeguard review. While these findings may be similar, their inclusion in either the POA&M or CAP is dependent upon how they were identified and who (the agency or the Office of Safeguards) is monitoring the finding resolution. Based upon deficiencies noted during the agency's inspection, list all deficiencies and corrective actions along with reasonable time frames for the remediation to occur* (refer to *Section 7.3, Corrective Action Plan*).

7.0 Reporting Requirements—6103(p)(4)(E)

7.1 General

IRC 6103(p)(4)(E) requires agencies receiving FTI to report on procedures established and used for ensuring the confidentiality of FTI that is received, processed, stored, or transmitted to or from the agency. The major components consisting of reporting requirements include the SSR, CAP and 45-day notification requirements.

Another measure IRS requires is internal inspections by the recipient agency. The purpose is to ensure that the security policies and procedures established by the agency to protect FTI are functioning, maintained and enforced. The agency must submit copies of these inspections to the IRS with the SSR (see *Section 7.2, Safeguard Security Report*). To provide an objective assessment, the inspection must be conducted by a function other than the using function.

7.1.1 Report Submission Instructions

Correspondence, reports, and attachments should be sent electronically to the Office of Safeguards using one of the following two methods:

- Secure Data Transfer (SDT), if the agency participates in the SDT program
- Email to Safeguards mailbox at SafeguardReports@irs.gov. Email transmissions must be sent by an IRS-approved encrypted method as outlined in *Section 7.1.2, Encryption Requirements*

Please adhere to the following guidelines when submitting correspondence, reports, and attachments to the Office of Safeguards:

- Submissions must be made using official templates provided by the Office of Safeguards
- If the report refers to external file attachments, the reference should clearly identify the filename and section contained within the attachment being referenced
- Attachments must be named clearly and identify the associated section in the SSR, CAP, or 45-day notification
- Attachment filenames must follow a standardized naming convention (e.g., CAPATT1, CAPATT2)
- Do not embed the attachment into the SSR, CAP, or 45-day notification

7.1.2 Encryption Requirements

The Office of Safeguards recommends that all required reports, when sent to the Office of Safeguards via email, be transmitted using IRS-approved encryption methods to protect sensitive information. Agencies are requested to adhere to the following guidelines to use encryption:

- Compress files in .zip or .zipx formats
- Encrypt the compressed file using Advanced Encryption Standard
- Use a strong 256-bit encryption key string
- Ensure a strong password or pass phrase is generated to encrypt the file
- Communicate the password or pass phrase with the Office of Safeguards through a separate email or via a telephone call to your IRS contact person. Do not provide the password or passphrase in the same email containing the encrypted attachment

Refer to your specific file compression software user guide for instructions on how to compress and encrypt files. Known compatible products with IRS include but are not limited to WinZip and Secure Zip.

Please remember, while the attachment is encrypted, the content of the email message will not be encrypted, so it is important that any sensitive information be contained in the attachment (encrypted document).

7.2 Safeguard Security Reports

Agencies executing data exchange agreements involving access to FTI and subject to safeguarding requirements must provide evidence that adequate safeguard protections and controls are in place before IRS will authorize the release of FTI. The agency must submit an initial SSR for approval at least 90 days prior to the agency planned date for receipt of FTI.

7.2.1 Initial SSR Submission Instructions – New Agency Responsibilities

In order to obtain initial IRS approval to receive FTI, an agency new to the Safeguard Program must have an approved SSR. To facilitate IRS approval, the agency is expected to:

- Designate an agency Safeguards point of contact (POC), see *Section 2.5 Coordinating Safeguards Within an Agency*
- Make program officials and/or contractors available to discuss access and use of FTI, as needed
- The SSR must be submitted for approval at least 90 days prior to the agency receiving FTI

IRS will request evidentiary documentation for the controls shown in the table below during review of the agency's SSR.

Table 5 - Evidentiary Requirements for SSR approval before release of FTI

800-53 Control	Control Name	Evidentiary Documents (Artifacts) for Review
Section 5.2	Comingling and Labeling	• Screenshots of database schemas that show electronic FTI labeling • Sample output (report/notice) that shows how FTI is labeled
AC-6	Least Privilege	• FTI data flow diagram (physical and logical) to include all devices and inputs/outputs • Access Control Policy & Procedures
AC-17	Remote Access	• Screenshot of authentication screens • Document how multi-factor authentication is deployed for all remote network access to systems containing FTI and the tokens used for authentication
AC-20	Use of External Information System	• Remote Access Policy & Procedures • Notice of Use for any non-agency-owned information systems; components; or devices to process, store, or transmit FTI, seeking IRS approval to meet 45-Day Notification Reporting Requirement
AU-2	Audit Events	• Audit and accountability policy and procedure for operating systems, databases and applications with FTI • Log Monitoring Policy (recordkeeping)
AU-3	Content of Audit Records	• Sample audit logs for all technologies/components associated with FTI
AT-4	Security Training Records	• Training material (for users and system security personnel) • Sample certification statement
CA-2	Security Assessments	• Independent Security Assessment Report (SAR) or other report reflecting the results of security testing and mitigation for any high findings within the last year.
CA-6	Security Authorization	• Signed Authority to Operate (ATO) for new systems (or DRAFT if ATO not yet granted) • Documentation appointing the system Authorization Official

CM-8	Information System Component Inventory	• Complete listing of FTI inventory (includes networking devices) identifying: platform, operating system, and applicable software
IA-5	Authenticator Management	• Password & Authenticator Management Policy & Procedures Screenshots of local security policy for password management
IR-6	Incident Reporting	• Incident Response Plan and Procedures
MP-6	Media Sanitization	• Media Sanitization Policy & Procedures • Destruction log template
PE-3	Physical Access Control	• Physical Access Policy & Procedures • Alternative Worksite Policy & Procedures
PE-8	Visitor Access Records	• Sample visitor access log
SA-9	External Information System Services	• System & Services Acquisition Policy and/or Access Control Policy
SC-4	Information in Shared Resources	• System & Communication Policy & Procedures
SC-7	Boundary Protection	• Network architecture and design documents and/or diagrams depicting FTI network segments or logical location of FTI system
SC-8	Transmission Confidentiality and Integrity	• System & Communication Policy & Procedures • Network design diagram and documentation with all FTI transmission protocols and encryption mechanisms identified
SI-2	Flaw Remediation	• Patch Management Policy & Procedure
SI-3	Malicious Code Protection	• Malicious Code Protection Policy & Procedure

If the agency does not submit all required evidentiary documentation, or the evidence is inadequate to comply with Pub 1075 standards, or the agency fails to conduct an independent security controls assessment, the IRS reserves the right to conduct an on-site visit to assess the effectiveness of the controls established in order to approve the SSR so FTI can be released. Subsequently, Safeguards will conduct a risk-based assessment to determine when to schedule an agency's first on-site safeguard review after initial receipt of FTI.

Refer to the SSR template on the Office of Safeguards website for additional guidance and instructions for completing the document.

7.2.2 Agencies Requesting New FTI Data Streams

The following documents need to be on file or submitted by an agency currently receiving FTI with an approved SSR and seeking additional FTI under newly assigned program authority or expanded statutory authority under IRC 6103. To obtain IRS approval to for a a new FTI data stream, the agency must have established compliance with existing safeguarding standards and have available for IRS will review:

- Approved SSR for the most recent reporting period
- Current CAP with approved mitigation strategies for critical and significant findings
- New FTI Data Stream need to be addressed in the next annual SSR update
- Documentation of security testing with any high findings mitigated and a signed ATO for any newly developed system that will be receiving, processing, storing or transmitting FTI (which is not covered in the agency's SSR already on file).

7.2.3 Annual SSR Update Submission Instructions

The agency must update and submit the SSR annually to encompass any changes that impact the protection of FTI. Example changes include, but are not limited to:

- New data exchange agreements
- New computer equipment, systems, or applications (hardware or software)
- New facilities including office moves and relocations
- Organizational changes, such as moving IT operations to a consolidated data center from an embedded IT operation

The following information must be updated in the SSR to reflect updates or changes regarding the agency or regarding safeguarding procedures within the reporting period:

- Changes to information or procedures previously reported
- Current annual period safeguard activities
- Planned actions affecting safeguard procedures
- Agency use of contractors (non-agency employees)

The annual SSR update must be submitted on the prior year SSR template that was returned to the agency. This will allow for a version control of the document, assurance that the agency addressed all outstanding items previously noted as well as reduce the need for recreating the entire document.

7.2.4 SSR Update Submission Dates

The SSR submission and all associated attachments must be sent annually to identify changes to safeguarding procedures. The annual update portion of the SSR should include a description of updates or changes that have occurred during the applicable reporting period. The CAP must also be submitted with the SSR (see *Section 7.3, Corrective Action Plan*, for additional CAP requirements).

Submission due dates are defined according to geographic locations or if the organization is a federal agency.

Table 6 – SSR Due Dates

	Reporting Period	SSR Due
Federal Agencies		
All Federal Agencies	January 1 through December 31	January 31
All State Agencies and Territories		
AK, AL, AR, AS, AZ, CA	February 1 through January 31	February 28
CNMI, CO, CT, DC, DE, FL, GA	March 1 through February 28	March 31
GU, HI, IA, ID, IL, IN, KS	April 1 through March 31	April 30
KY, LA, MA, MD, ME, MI	May 1 through April 30	May 31
MN, MO, MS, MT, NE	June 1 through May 31	June 30
NC, NH, NJ, NM, NV, NY	July 1 through June 30	July 31
ND, OH, OK, OR	August 1 through July 31	August 31
PA, PR, RI, SC, SD, TN	September 1 through August 31	September 30
TX, UT, VA, VI, VT, WA	October 1 through September 30	October 31
WI, WV, WY	November 1 through October 31	November 30

Educational institutions receiving IRS addresses to locate debtors under IRC 6103(m)(4)(B) must send annual reports to the Department of Education as the federal oversight agency for this program.

When extenuating circumstances exist, agencies may request an Annual SSR extension, in 30 day increments, for a maximum of 60 days. Extension requests should be submitted not later than (NLT) 30 days prior to the scheduled SSR due date. Request for extensions will not be considered after the scheduled SSR due date. A request for a second extension must be accompanied by a draft SSR.

Extension requests should be sent to the Office of Safeguards via Secure Data Transfer (SDT) or email to SafeguardReports@irs.gov, with the subject SSR extension request and reasons for the request. All extension requests will be evaluated on a case by case basis. Safeguards will provide an email response, approving or disapproving the request within 5 work days after receipt of the request.

7.3 Corrective Action Plan

The CAP represents the corrective actions described in the SRR. The IRS will provide each agency an SRR along with a CAP upon completion of an on-site review. The agency must develop the CAP to report on completed corrective actions as well as provide status updates to any unresolved or planned actions.

7.3.1 CAP Submission Instructions and Submission Dates

The agency must submit the CAP semi-annually, as an attachment to the SSR and on the CAP due date, which is six months from the scheduled SSR due date.

The CAP due dates are provided in the following chart.

Table 7 – CAP Due Dates

	CAP with SSR	CAP (only)
Federal Agencies		
All Federal Agencies	January 31	July 31
All State Agencies and Territories		
AK, AL, AR, AS, AZ, CA	February 28	August 31
CNMI, CO, CT, DC, DE, FL, GA	March 31	September 30
GU, HI, IA, ID, IL, IN, KS	April 30	October 31
KY, LA, MA, MD, ME, MI	May 30	November 30
MN, MO, MS, MT, NE	June 30	December 31
NC, NH, NJ, NM, NV, NY	July 31	January 31
ND, OH, OK, OR	August 31	February 28
PA, PR, RI, SC, SD, TN	September 30	March 31
TX, UT, VA, VI, VT, WA	October 31	April 30
WI, WV, WY	November 30	May 31

If the SRR was issued within 60 days from the upcoming CAP due date in the preceding chart, 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.

When extenuating circumstances exist, agencies may request an extension for no more than 30 days. Extension requests should be submitted not later than (NLT) 30 days prior to the scheduled CAP due date. Request for extensions will not be considered after the scheduled CAP due date. Extension requests should be sent to the Office of Safeguards via Secure Data Transfer (SDT) or email to SafeguardReports@irs.gov, with the subject CAP extension request and reasons for the request. All extension requests will be evaluated on a case by case basis. Safeguards will provide an email response, approving or disapproving the request within 5 work days after receipt of the request.

The CAP must be returned/submitted using the version sent by the Office of Safeguards with the SSR. The template should not be altered. The Planned Implementation Dates fields should not include any text; only numeric value and entered in mm/dd/yyyy format.

7.4 45-Day Notification Reporting Requirements

IRC 6103 limits the usage of FTI to only those purposes explicitly stated. Due to the security implications, higher risk of unauthorized disclosure and potential for unauthorized use of FTI based on specific activities conducted, the Office of Safeguards requires advanced notification (45 days) prior to implementing certain operations or technology capabilities that require additional uses of the FTI.

In addition to the initial receipt of FTI (see Section 2.1), the following circumstances or technology implementations require the agency to submit to the Office of Safeguards via the Office of Safeguards mailbox, at a minimum of 45 days ahead of the planned implementation, notification for the following activities that involve FTI:

Table 8 – 45-Day Notification Reporting Requirements

FTI related to:	Advance approval required to proceed?
Cloud Computing	No, only notification required*
Consolidated Data Center	No, only notification required*
Disclosure to a Contractor	No, Notification is required before releasing FTI to any agency contractor not listed in the last annual SSR. Only applicable for agencies specifically authorized pursuant to IRC 6103 statute or regulation.*
Re-disclosure by Contractor to Sub-Contractor	Yes, FTI may not be released to a sub-contractor absent IRS approval in writing from Safeguards. Only applicable for agencies specifically authorized pursuant to IRC 6103 statute or regulation.*
Data Warehouse Processing	No
Non-Agency-Owned Information Systems	No
Tax Modeling for Tax Administration	Yes, by Disclosure
Test Environment	Yes, by Safeguards
Virtualization of IT Systems	No

See additional details pertaining to each topic in the following sections. Contact the Office of Safeguards mailbox with any questions pertaining to the 45-day notification requirement.

7.4.1 Cloud Computing

Receiving, processing, storing, or transmitting FTI in a cloud environment requires prior notification to the Office of Safeguards. Refer to *Section 9.4.1, Cloud Computing Environments*, for guidance and details on 45-day notification requirements.
*Note: Advance *approval* is not required, only advance notification.

7.4.2 Consolidated Data Center

Agencies are required to notify the Office of Safeguards when moving IT operations to a consolidated data center. Refer to *Section 5.4.2, Contractor- or Agency-Shared Facility—Consolidated Data Centers* for additional information.
*Note: Advance *approval* is not required, only advance notification.

7.4.3 Contractor or Subcontractor Access

All agencies intending to re-disclose FTI to contractors must notify the IRS at least 45 days prior to the planned re-disclosure. Contractors consist of but are not limited to cloud computing providers, consolidated data centers, off-site storage facilities, shred companies, IT support, or tax modeling/revenue forecasting providers. The contractor notification requirement also applies in the circumstance where the contractor hires additional subcontractor services. Approval is required if the (prime) contractor hires additional subcontractor services in accordance with *Exhibit 6, Contractor 45-Day Notification Procedures.*

> *Notification is also required for contractors to perform statistical analysis, tax modeling, or revenue projections (*see *Section 2.4, State Tax Agency Limitations).*

7.4.4 Data Warehouse Processing

No prior notification is required when an agency implements a data warehouse containing FTI. For additional data warehouse guidance, see *Exhibit 10, Data Warehouse Security Requirements.*

7.4.5 Non-Agency-Owned Information Systems

Under limited circumstances, the IRS may review requests for the use or access to FTI using a non-agency-owned information system (e.g., mobile devices, cloud environments, outsourced data centers). Notify the Office of Safeguards 45 days in advance of planned activities to use non-agency-owned information systems to receive, process, store, or transmit FTI. See *Section 9.3.1.15 Use of External Information Systems (AC-20)* for additional information.

7.4.6 Tax Modeling

The agency must notify the Office of Safeguards if planning to include FTI in statistical analysis, tax modeling, or revenue projections.

The Office of Safeguards will forward the notification to the IRS Statistics of Income for approval of the modeling methodology (see *Section 2.4, State Tax Agency Limitations*).

7.4.7 Live Data Testing

Agencies must submit a Data Testing Request (DTR) form to request approval to use live FTI in a testing environment. Refer to *Section 9.4.6, Live Data Testing*, for additional guidance on 45-day notification requirements.

7.4.8 Virtualization of Information Technology Systems

No prior notification is required when an agency is planning to receive, process, store, or transmit FTI in virtualized environments. For additional guidance, see *Section 9.4.14, Virtualization Environments.*

8.0 Disposing of FTI—IRC 6103(p)(4)(F)

8.1 General

Users of FTI are required by IRC 6103(p)(4)(F) to take certain actions after using FTI to protect its confidentiality (see *Exhibit 2, USC Title 26, IRC 6103(p)(4)*, and *Exhibit 5, Civil Damages for Unauthorized Disclosure*). Agency officials and employees either will return the information (including any copies made) to the office from which it was originally obtained or destroy the FTI. Agencies will include in their annual report (e.g., SSR) a description of the procedures implemented. See *Section 7.0, Reporting Requirements—6103(p)(4)(E)* for additional reporting requirements.

8.2 Returning IRS Information to the Source

Agencies electing to return IRS information must use a receipt process and ensure that the confidentiality is protected at all times during transport (see *Section 4.4, FTI in Transit*).

8.3 Destruction and Disposal

FTI furnished to the user and any paper material generated therefrom, such as copies, photo impressions, computer printouts, notes, and work papers, must be destroyed by burning or shredding. If a method other than burning or shredding is used, that method must make the FTI unreadable or unusable.

The following guidelines must be observed when destroying FTI:

Table 9 – FTI Destruction Methods

Burning
The material must be burned in an incinerator that produces enough heat to burn the entire bundle, or the bundle must be separated to ensure that all pages are incinerated.

Shredding
To make reconstruction more difficult: • Destroy paper using cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen. *If shredding deviates from the above specification, FTI must be safeguarded until it reaches the stage where it is rendered unreadable through additional means, such as burning or pulping.*

FTI furnished or stored in electronic format must be destroyed in the following manner:

- Electronic media (e.g., hard drives, tapes, CDs, and flash media) must be destroyed according to guidance in *Section 9.3.10.6, Media Sanitization (MP-6)*, and *Section 9.4.7, Media Sanitization*. Electronic media containing FTI must not be made available for reuse by other offices or released for destruction without first being subjected to electromagnetic erasing. If reuse is not intended, the tape must be destroyed by burning or shredding in accordance with applicable standards (see Table 13, Media Sanitation Techniques).

- Destroy microfilms (microfilm, microfiche, or other reduced image photo negatives) by burning.

Whenever physical media leaves the physical or systemic control of the agency for maintenance, exchange, or other servicing, any FTI on it must be destroyed by sanitizing according to guidance in *Section 9.3.10.6, Media Sanitization (MP-6)*, and *Section 9.4.7, Media Sanitization*. FTI must be purged from the media prior to allowing release.

When using either method for destruction, every third piece of physical electronic media must be checked to ensure appropriate destruction of FTI.

Hand tearing, recycling, or burying information in a landfill are unacceptable methods of disposal.

8.4 Other Precautions

FTI must never be disclosed to an agency's agents or contractors during disposal without legal authorization and destruction must be witnessed by an agency employee.

The Department of Justice, state tax agencies, and SSA may be exempted from the requirement of having agency personnel witness destruction by a contractor. If a contractor is used:

- The contract must contain safeguard language in *Exhibit 7, Safeguarding Contract Language* as appropriate to the contract to ensure the protection of FTI.
- Destruction of FTI must be certified by the contractor when not witnessed by an agency employee.
- It is recommended that the agency periodically observe the process to ensure compliance with security of FTI until it reaches a non-disclosable state and that an approved destruction method is utilized.
- If the agency has legal authority to disclose FTI to a disposal contractor and chooses one that is National Association for Information Destruction (NAID) certified, the agency will not be required to complete an internal inspection every 18 months of that facility. However, it must maintain a copy of, and periodically validate the NAID certification.

9.0 Computer System Security

9.1 General

This section details the computer security requirements agencies must meet to adequately protect FTI under their administrative control. While the Office of Safeguards has responsibility to ensure the protection of FTI, it is the responsibility of the agency to build in effective security controls into its own IT infrastructure to ensure that FTI is protected at all points where it is received, processed, stored, or transmitted. It will not be the intent of IRS to monitor each control identified but to provide these to the organization, identifying those controls required for the protection of moderate risk systems within the federal government.

All agency information systems used for receiving, processing, storing, or transmitting FTI must be hardened in accordance with the requirements in this publication. Agency information systems include the equipment, facilities, and people that collect, process, store, display, and disseminate information. This includes computers, hardware, software, and communications, as well as policies and procedures for their use.

Impact levels used in this document are described in Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. NIST publications are available at http://csrc.nist.gov/publications/PubsSPs.html.

The computer security framework was primarily developed using guidelines specified in NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* and NIST SP 800- 53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Only applicable NIST SP 800-53 controls are included in this publication as a baseline. Applicability was determined by selecting controls required to protect the confidentiality of FTI. Agencies are encouraged to review supplemental guidance provided within NIST SP 800-53.

Section 9.3, NIST SP 800-53 Control Requirements, provides the security control requirements that relate to protecting information systems that receive, process, store, or transmit FTI and are based on the moderate baseline security controls defined by NIST.

The Office of Safeguards has included NIST control enhancement requirements where appropriate to protect the confidentiality of FTI. Control enhancements are identified with a CE designator after the requirement is described.

9.2 Assessment Process

The Office of Safeguards will assess agency compliance with the computer security requirements identified in this publication as part of the on-site review process. Requirements are assessed as they related to NIST SP 800-53 security controls as outlined in this publication. Please see *Section 2.7.2 Computer Security Review Process* for information on the on-site review process.

9.3 NIST SP 800-53 Control Requirements

9.3.1 Access Control

9.3.1.1 Access Control Policy and Procedures (AC-1)

The agency must:

a) Develop, document, and disseminate to designated agency officials:
   (1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
   (2) Procedures to facilitate the implementation of the access control policy and associated access controls

b) Review and update the current:
   (1) Access control policy every three years (or if there is a significant change)
   (2) Access control procedures at least annually

9.3.1.2 Account Management (AC-2)

The agency must:

a. Identify and select the accounts with access to FTI to support agency missions/business functions
b. Assign account managers for information system accounts;
c. Establish conditions for group and role membership
d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account
e. Require approval for requests to create information system accounts
f. Create, enable, modify, disable, and remove information system accounts in accordance with documented agency account management procedures
g. Monitor the use of information system accounts
h. Notify account managers when accounts are no longer required, when users are terminated or transferred, or when individual information system usage or need- to-know permission changes
i. Authorize access to information systems that receive, process, store, or transmit FTI based on a valid access authorization, need-to-know permission, and under the authority to re-disclosed FTI under the provisions of IRC 6103
j. Review accounts for compliance with account management requirements at a
k. minimum of annually for user accounts and semi-annually for privileged accounts
l. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

The information system must automatically disable inactive accounts after 120 days of inactivity. (CE3)

9.3.1.3 Access Enforcement (AC-3)

The information system must enforce:

a) Approved authorizations for logical access to information and system resources in accordance with applicable access control policies
b) A role-based access control policy over defined subjects and objects and controls access to FTI based upon a valid access authorization, intended system usage, and the authority to be disclosed FTI under the provisions of IRC 6103

9.3.1.4 Information Flow Enforcement (AC-4)

The information system must enforce approved authorizations for controlling the flow of FTI within the system and between interconnected systems based on the technical safeguards in place to protect the FTI.

Additional requirements for protecting the flow of FTI can be found in:

- *Section 9.4.3, Email Communications*
- *Section 9.4.4, Fax Equipment*
- *Section 9.4.9, Multi-Functional Devices*

9.3.1.5 Separation of Duties (AC-5)

The agency must:

a. Separate duties of individuals to prevent harmful activity without collusion
b. Document separation of duties of individuals
c. Define information system access authorizations to support separation of duties

9.3.1.6 Least Privilege (AC-6)

The agency must:

a. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with agency missions and business functions
b. Explicitly authorize access to FTI (CE1)
c. Require that users of information system accounts, or roles, with access to FTI, use non-privileged accounts or roles when accessing non-security functions (CE2)
d. Restrict privileged accounts on the information system to a limited number of individuals with a need to perform administrative duties (CE5)

The information system must:

a. Audit the execution of privileged functions (CE9)
b. Prevent non-privileged users from executing privileged functions; including disabling, circumventing, or altering implemented security safeguards/countermeasures (CE10)

9.3.1.7 Unsuccessful Logon Attempts (AC-7)

The information system must:

a. Enforce a limit of three consecutive invalid logon attempts by a user during a 120-minute period
b. Automatically lock the account for a period of at least 15 minutes

Specific to mobile device requirements, the logon is to the mobile device, not to any one account on the device. Additional mobile device controls are addressed in *Section 9.3.1.14, Access Control for Mobile Devices (AC-19),* and *Section 9.4.8, Mobile Devices.*

9.3.1.8 System Use Notification (AC-8)

The information system must:

a. Before granting access to the system, display to users an IRS-approved warning banner that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

    1. The system contains U.S. Government information
    2. Users actions are monitored and audited
    3. Unauthorized use of the system is prohibited
    4. Unauthorized use of the system is subject to criminal and civil sanctions

    The warning banner must be applied at the application, database, operating system, and network device levels for all systems that receive, process, store, or transmit FTI.

b. Retain the warning banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

For publicly accessible systems, the information system must:

a. Display the IRS-approved warning banner granting further access
b. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities
c. Include a description of the authorized uses of the system

For sample warning banners approved by the Office of Safeguards, see Exhibit 8.

9.3.1.9 Session Lock (AC-11)

The information system must:

a. Prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user
b. Retain the session lock until the user reestablishes access using established identification and authentication procedures

9.3.1.10 Session Termination (AC-12)

The information system must automatically terminate a user session after 30 minutes of inactivity.

> *This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system.*

9.3.1.11 Permitted Actions without Identification or Authentication (AC-14)

The agency must:

a. Identify specific user actions that can be performed on the information system without identification or authentication consistent with agency missions/business functions. FTI may not be disclosed to individuals on the information system without identification and authentication
b. Document and provide supporting rationale in the SSR for the information system the user actions not requiring identification or authentication

> *Examples of access without identification and authentication would be instances in which the agency maintains a publicly accessible website for which no authentication is required.*

9.3.1.12 Remote Access (AC-17)

The agency must:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed
b. Authorize remote access to the information system prior to allowing such connections
c. Authorize and document the execution of privileged commands and access to security-relevant information via remote access for compelling operational needs only (CE4)

The information system must:

a. Monitor and control remote access methods (CE1)
b. Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions where FTI is transmitted over the remote connection and (CE2)
c. Route all remote accesses through a limited number of managed network access control points (CE3)

Remote access is defined as any access to an agency information system by a user communicating through an external network, for example, the Internet.

Any remote access where FTI is accessed over the remote connection must be performed using multi-factor authentication.

FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies, or military installations. Further, FTI may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore.

9.3.1.13 Wireless Access (AC-18)

The agency must:

a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access
b. Authorize wireless access to the information system prior to allowing such connections
c. Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system (SI-4, CE14)

The information system must protect wireless access to the system using authentication and encryption. (CE1)

Additional requirements for protecting FTI on wireless networks are provided in *Section 9.4.18, Wireless Networks*.

9.3.1.14 Access Control for Mobile Devices (AC-19)

A mobile device is a computing device that (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable, or removable data storage; and (iv) includes a self-contained power source.

The agency must:

a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for agency-controlled mobile devices
b. Authorize the connection of mobile devices to agency information systems
c. Employ encryption to protect the confidentiality and integrity of information on mobile devices (e.g., smartphones and laptop computers) (CE5)
b. Purge/wipe information from mobile devices based on 10 consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones and tablets). Laptop computers are excluded from this requirement (AC-7, CE2)

Additional requirements on protecting FTI accessed by mobile devices are provided in *Section 9.4.8, Mobile Devices*.

9.3.1.15 Use of External Information Systems (AC-20)

Unless approved by the Office of Safeguards, the agency must prohibit:

a. Access to FTI from external information systems, other than through a virtual desktop infrastructure (see *Section 9.4.13 Virtual Desktop Infrastructure*)
b. Use of agency-controlled portable storage devices (e.g., flash drives, external hard drives) containing FTI on external information systems (CE2)
c. Use of non-agency-owned information systems; system components; or devices to process, store, or transmit FTI; any non-agency-owned information system usage requires the agency to notify the Office of Safeguards 45 days prior to implementation (see Section 7.4, *45-Day Notification Reporting Requirements)* (CE3)

The agency may allow the use of personally-owned devices, without notification, only for the following purposes:

a. Bring Your Own Device (BYOD) used to access e-mail, where all requirements in Section 9.4.8 Mobile Devices are met
b. Remote access through a virtual desktop infrastructure (VDI) environment, where all requirements in Section 9.4.13 Virtual Desktop Infrastructure are met

External information systems, or non-agency-owned equipment, include any technology used to receive, process, transmit, or store FTI that is not owned and managed by the agency. A subset of external information systems is personally-owned devices, which include any device owned by an individual employee, rather than the agency itself.

9.3.1.16 Information Sharing (AC-21)

The agency must restrict the sharing/re-disclosure of FTI to only those authorized in IRC 6103 and as approved by the Office of Safeguards.

9.3.1.17 Publicly Accessible Content (AC-22)

The agency must:

a. Designate individuals authorized to post information onto a publicly accessible information system
b. Train authorized individuals to ensure that publicly accessible information does not contain FTI
c. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that FTI is not included
d. Review the content on the publicly accessible information system for FTI, at a minimum, quarterly and remove such information, if discovered

9.3.2 Awareness and Training

9.3.2.1 Security Awareness and Training Policy and Procedures (AT-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:

    1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls

b. Review and update the current:

    1. Security awareness and training policy every three years (or if there is a significant change)
    2. Security awareness and training procedures at least annually

9.3.2.2 Security Awareness Training (AT-2)

The agency must:

a. Provide basic security awareness training to information system users (including managers, senior executives, and contractors):

    1. As part of initial training for new users
    2. When required by information system changes
    3. At least annually thereafter

b. Include security awareness training on recognizing and reporting potential indicators of insider threat. (CE2)

This section is closely coupled with Section 6.3, Disclosure Awareness Training, which provides the requirement for general FTI disclosure awareness training; however, this control is focused on information security and operational security awareness.

Insider threat training should bring awareness of the potential for individuals (e.g., employees, contractors, former employees) to use insider knowledge of sensitive agency information (e.g., security practices, systems that hold sensitive data) to perform malicious actions, which could include the unauthorized access or re-disclosure of FTI.

9.3.2.3 Role-Based Security Training (AT-3)

The agency must provide role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties that require access to FTI
b. When required by information system changes
c. At least annually thereafter

Personnel with security roles and responsibilities include, but are not limited to, the following positions: Information System Security Manager, Information System Security Officer, Security Specialist, Network Administrator, Systems Administrator, Database Administrator, Programmer/Systems Analyst, System Owner, Systems Designer/Systems Developer, helpdesk.

Note: Training conducted under this section is distinct from Section 6.3, Disclosure Awareness, and Section 9.3.2.2, Security Awareness Training (AT-2).

9.3.2.4 Security Training Records (AT-4)

The agency must:

a. Document and monitor individual information system security training activities, including basic security awareness training and specific information system security training
b. Retain individual training records for a period of five years

9.3.3 Audit and Accountability

9.3.3.1 Audit and Accountability Policy and Procedures (AU-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance

2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls

b. Review and update the current:

1. Audit and accountability policy every three years
2. Audit and accountability procedures at least annually.

9.3.3.2 Audit Events (AU-2)

Security-relevant events must enable the detection of unauthorized access to FTI data. Auditing must be enabled to the greatest extent necessary to capture access, modification, deletion, and movement of FTI by each unique user.

The agency must:

a. Determine that the information system is capable, at a minimum, of auditing the following event types:
   1. Log onto system
   2. Log off of system
   3. Change of password
   4. All system administrator commands, while logged on as system administrator
   5. Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS)
   6. Creation or modification of super-user groups
   7. Subset of security administrator commands, while logged on in the security administrator role
   8. Subset of system administrator commands, while logged on in the user role
   9. Clearing of the audit log file
   10. Startup and shutdown of audit functions
   11. Use of identification and authentication mechanisms (e.g., user ID and password)
   12. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su)
   13. Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system
   14. Changes made to an application or database by a batch file
   15. Application-critical record changes
   16. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility)
   17. All system and data interactions concerning FTI
   18. Additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards website
b. Coordinate the security audit function with other agency entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events
c. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents
d. Review and update the audited events at a minimum, annually (CE3)

Access to FTI must be audited at the operating system, software, and database levels. Software and platforms have differing audit capabilities. Each individual platform audit capabilities and requirements are maintained on the platform-specific Office of Safeguards SCSEM, which is available on the IRS Office of Safeguards website.

9.3.3.3 Content of Audit Records (AU-3)

The information system must:

a. Generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event
b. Generate audit records containing details to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected in the audit records for audit events identified by type, location, or subject (CE1)

9.3.3.4 Audit Storage Capacity (AU-4)

The agency must allocate audit record storage capacity to retain audit records for the required audit retention period of seven years.

9.3.3.5 Response to Audit Processing Failures (AU-5)

The information system must:

a. Alert designated agency officials in the event of an audit processing failure
b. Monitor system operational status using operating system or system audit logs and verify functions and performance of the system. Logs shall be able to identify where system process failures have taken place and provide information relative to corrective actions to be taken by the system administrator
c. Provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity (CE1)

9.3.3.6 Audit Review, Analysis, and Reporting (AU-6)

The agency must:

a. Review and analyze information system audit records at least weekly or more frequently at the discretion of the information system owner for indications of unusual activity related to potential unauthorized FTI access
b. Report findings according to the agency incident response policy. If the finding involves a potential unauthorized disclosure of FTI, the appropriate special agent-in-charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards must be contacted, as described in *Section 10.0, Reporting Improper Inspections or Disclosures*.

The Office of Safeguards recommends agencies identify events that may indicate a potential unauthorized access to FTI. This recommendation is not a requirement at this time, but agencies are encouraged to contact the Office of Safeguards with any questions regarding implementation strategies. Methods of detecting unauthorized access to FTI include matching audit trails to access attempts (successful or unsuccessful) across the following categories:

Table 10 – Proactive Auditing Methods to Detect Unauthorized Access to FTI

Do Not Access List	Create a Do Not Access list to identify high-profile individuals or companies whose records have a high probability of being accessed without proper authorization
Time of Day Access	Identify suspicious behavior by tracking FTI accesses outside normal business hours
Name Searches	Detect potential unauthorized access by monitoring name searches (especially searches on the same last name as the employee)
Previous Accesses	Identify employee accesses to Tax Identification Numbers (TINs) that the employee has accessed in the past but currently does not have a case assignment or need to access
Volume	Monitor the volume of accesses a person performs and compare them to past case assignment levels
Zip Code	Determine whether an employee is accessing taxpayers whose address of record is geographically close to the employee's home or work location (i.e., same building, zip code, block)
Restricted TIN	Monitor all TINs associated with past employees' tax returns (e.g., self, spouse, children, businesses).

It is recommended the agency define a frequency in which the preceding categories are updated for an individual to ensure the information is kept current.

9.3.3.7 Audit Reduction and Report Generation (AU-7)

The information system must provide an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
b. Does not alter the original content or time ordering of audit records.

9.3.3.8 Time Stamps (AU-8)

The information system must:

a. Use internal system clocks to generate time stamps for audit records
b. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT)
c. Compare and synchronize the internal information system clocks to an enterprise-wide authoritative time source. Where possible, synchronize enterprise time source to an external source (e.g., NIST, Naval Observatory).

9.3.3.9 Protection of Audit Information (AU-9)

The information system must protect audit information and audit tools from unauthorized access, modification, and deletion.

The agency must authorize access to manage audit functionality only to designated security administrator(s) or staff other than the system and network administrator. System and network administrators must not have the ability to modify or delete audit log entries. (CE4)

9.3.3.10 Audit Record Retention (AU-11)

The agency must retain audit records for the events identified in Section 9.3.3.2, Audit Events (AU-2) for seven years to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements.

9.3.3.11 Audit Generation (AU-12)

The information system must:

a. Provide audit record generation capability for the auditable events defined in *Section 9.3.3.2, Audit Events (AU-2)*
b. Allow designated agency officials to select which auditable events are to be audited by specific components of the information system
c. Generate audit records for the events with the content defined in *Section 9.3.3.4, Content of Audit Records (AU-3).*

9.3.3.12 Cross-Agency Auditing (AU-16)

The agency must employ mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across agency boundaries.

> *This requirement applies to outsourced data centers or cloud providers. The provider must be held accountable to protect and share audit information with the agency through the contract.*

See *Section 9.4.1, Cloud Computing Environments* for additional cloud computing requirements, including language for cloud computing requirements. Also see *Section 5.4, Controls over Processing* for information pertaining to consolidated data centers.

9.3.4 Security Assessment and Authorization

9.3.4.1 Security Assessment and Authorization Policy and Procedures (CA-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls

b. Review and update the current:
    1. Security assessment and authorization policy every three years
    2. Security assessment and authorization procedures at least annually

9.3.4.2 Security Assessments (CA-2)

The agency must:

a. Develop a security assessment plan that describes the scope of the assessment, including:
    1. Security controls and control enhancements under assessment
    2. Assessment procedures to be used to determine security control effectiveness
    3. Assessment environment, assessment team, and assessment roles and responsibilities

b. Assess the security controls in the information system and its environment at a minimum on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements

c. Produce a security assessment report that documents the results of the assessment
d. Provide the results of the security control assessment to the agency's Authorizing Official

9.3.4.3 System Interconnections (CA-3)

The agency must:

a. Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements
b. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated
c. Review and update the system interconnection on an annual basis
d. Employ deny-all and allow-by-exception policy for allowing systems that receive, process, store, or transmit FTI to connect to external information systems (CE5)

9.3.4.4 Plan of Action and Milestones (CA-5)

The agency must:

a. Develop a POA&M for the information system to document the agency's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system
b. Update the existing POA&M on a quarterly basis, at a minimum, based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities

The POA&M must comprise of an all-inclusive tool or document for the agency to track vulnerabilities identified by the self-assessments, internal inspections, external audits and any other vulnerabilities identified for information systems that receive, process, store, or transmit FTI.

Additional information is available in *Section 6.5, Plan of Action and Milestones*.

9.3.4.5 Security Authorization (CA-6)

The agency must:

a. Assign a senior-level executive or manager as the authorizing official for the information system
b. Ensure that the authorizing official authorizes the information system for processing before commencing operations
c. Update the security authorization whenever there is a significant change to the system, or every three years, whichever occurs first

9.3.4.6 Continuous Monitoring (CA-7)

The agency must develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

a. Establishment of agency-defined metrics to be monitored annually, at a minimum
b. Ongoing security control assessments in accordance with the agency continuous monitoring strategy
c. Ongoing security status monitoring of agency-defined metrics in accordance with the agency continuous monitoring strategy

9.3.5 Configuration Management

9.3.5.1 Configuration Management Policy and Procedures (CM-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls
b. Review and update the current:
    1. Configuration management policy every three years
    2. Configuration management procedures at least annually

9.3.5.2 Baseline Configuration (CM-2)

The agency must develop, document, and maintain under configuration control, a current baseline configuration of the information system.

The agency must review and update the baseline configuration of the information system: (CE1)

a. At a minimum annually
b. When required due to system upgrades, patches, or other significant changes
c. As an integral part of information system component installations and upgrades

The Office of Safeguards recommends using SCSEMs provided on the Office of Safeguards website for developing an information system baseline configuration.

9.3.5.3 Configuration Change Control (CM-3)

The agency must:

a. Determine the types of changes to the information system that are configuration controlled
b. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses
c. Document configuration change decisions associated with the information system
d. Implement approved configuration-controlled changes to the information system
e. Retain records of configuration-controlled changes to the information system for the life of the system
f. Audit and review activities associated with configuration-controlled changes to the information system
g. Coordinate and provide oversight for configuration change control activities through a Configuration Control Board that convenes when configuration changes occur
h. Test, validate, and document changes to the information system before implementing the changes on the operational system (CE2)

9.3.5.4 Security Impact Analysis (CM-4)

The agency must analyze changes to the information system to determine potential security impacts prior to change implementation.

9.3.5.5 Access Restrictions for Change (CM-5)

The agency must define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

9.3.5.6 Configuration Settings (CM-6)

The agency must:

a. Establish and document configuration settings for IT products that receive, process, store, or transmit FTI using Office of Safeguards–approved compliance requirements (e.g., SCSEMs, assessment tools) that reflect the most restrictive mode consistent with operational requirements
b. Implement the configuration settings
c. Identify, document, and approve any deviations from established configuration settings for information systems that receive, process, store, or transmit FTI
d. Monitor and control changes to the configuration settings in accordance with agency policies and procedures

The authoritative source for platform checklists used by the Office of Safeguards is the NIST Checklist Program Repository (http://checklists.nist.gov). Office of Safeguards SCSEMs may include compliance requirements from one or more of the following security benchmarks:

- *United States Government Configuration Baseline (USGCB)*
- *Center for Internet Security (CIS) Benchmarks*
- *Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS)*
- *National Security Agency (NSA) Configuration Guides*

9.3.5.7 Least Functionality (CM-7)

The agency must:

a. Configure the information system to provide only essential capabilities
b. Prohibit or restrict the use of the functions, ports, protocols, or services as defined in Office of Safeguards–approved compliance requirements (e.g., SCSEMs, assessment tools)
c. Review the information system as part of vulnerability assessments to identify unnecessary or non-secure functions, ports, protocols, and services (see *Section 9.3.14.3, Vulnerability Scanning (RA-5)*)
d. Disable defined functions, ports, protocols, and services within the information system deemed to be unnecessary or non-secure

9.3.5.8 Information System Component Inventory (CM-8)

The agency must:

a. Develop and document an inventory of information system components that:
    1. Accurately reflects the current information system
    2. Includes all components that store, process, or transmit FTI
    3. Is at the level of granularity deemed necessary for tracking and reporting
    4. Includes information deemed necessary to achieve effective information system component accountability
b. Review and update the information system component inventory through periodic manual inventory checks or a network monitoring tool that automatically maintains the inventory
c. Update the inventory of information system components as an integral part of component installations, removals, and information system updates (CE1)

Additional requirements for maintaining a system component inventory are provided in *Section 9.4.12, System Component Inventory*, as well as *NIST SP 800-70 Security Configuration Checklists Program for IT Products- Guidance for Checklists Users and Developers.*

9.3.5.9 Configuration Management Plan (CM-9)

The agency must develop, document, and implement a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures
b. Establishes a process for identifying configuration items throughout the system development life cycle (SDLC) and for managing the configuration of the configuration items
c. Defines the configuration items for the information system and places the configuration items under configuration management
d. Protects the configuration management plan from unauthorized disclosure and modification

9.3.5.10 Software Usage Restrictions (CM-10)

The agency must:

a. Use software and associated documentation in accordance with contract agreements and copyright laws
b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution
c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work

The agency must establish restrictions on the use of open source software. Open source software must: (CE1)

a. Be legally licensed
b. Approved by the agency IT department
c. Adhere to a secure configuration baseline checklist from the U.S. Government or industry

9.3.5.11 User-Installed Software (CM-11)

The agency must:

a. Establish policies governing the installation of software by users
b. Enforce software installation policies through automated methods
c. Monitor policy compliance on a continual basis

9.3.6 Contingency Planning

All FTI that is transmitted to agencies is backed up and protected within IRS facilities. As such, the focus of contingency planning controls is on the protection of FTI stored in backup media or used at alternative facilities and not focused on the availability of data. Agencies must develop applicable contingencies for ensuring that FTI is available, based upon their individual risk-based approaches.

9.3.6.1 Contingency Planning Policy and Procedures (CP-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls
b. Review and update the current:
    1. Contingency planning policy every three years
    2. Contingency planning procedures at least annually

9.3.6.2 Contingency Plan (CP-2)

The agency must:

a. Develop a contingency plan for the information system that:
    1. Identifies essential missions and business functions and associated contingency requirements
    2. Provides recovery objectives, restoration priorities, and metrics
    3. Addresses contingency roles, responsibilities, and assigned individuals with contact information
    4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure
    5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented
    6. Is reviewed and approved by designated agency officials
b. Distribute copies of the contingency plan to key contingency personnel
c. Coordinate contingency planning activities with incident handling activities
d. Review the contingency plan for the information system at least annually

e. Update the contingency plan to address changes to the agency, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing
f. Communicate contingency plan changes to key contingency personnel
g. Protect the contingency plan from unauthorized disclosure and modification

9.3.6.3 Contingency Training (CP-3)

The agency must provide contingency training to information system users consistent with assigned roles and responsibilities:

a. Prior to assuming a contingency role or responsibility
b. When required by information system changes
c. Annually thereafter

9.3.6.4 Contingency Plan Testing (CP-4)

The agency must:

a. Test the contingency plan for the information system, at a minimum annually, to determine the effectiveness of the plan and the agency's readiness to execute the plan
b. Review the contingency plan test results
c. Initiate corrective actions, if needed

9.3.6.5 Alternate Storage Site (CP-6)

The agency must:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of information system backup information
b. Ensure that the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103

9.3.6.6 Alternate Processing Site (CP-7)

The agency must:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of information system operations, in accordance with the agency's contingency plan when the primary processing capabilities are unavailable
b. Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the agency-defined time period for transfer/resumption

c. Ensure that the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103

9.3.6.7 Information System Backup (CP-9)

The agency must:

a. Conduct backups of user-level information, system-level information, and security-related documentation consistent with the defined frequency in the agency's contingency plan
b. Protect the confidentiality of backup information at storage locations pursuant to IRC 6103 requirements

9.3.6.8 Information System Recovery and Reconstitution (CP-10)

The agency must provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

9.3.7 Identification and Authentication

9.3.7.1 Identification and Authentication Policy and Procedures (IA-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls
b. Review and update the current:
    1. Identification and authentication policy every three years
    2. Identification and authentication procedures at least annually

9.3.7.2 Identification and Authentication (Organizational Users) (IA-2)

The information system must:

a. Uniquely identify and authenticate agency users (or processes acting on behalf of agency users)
b. Implement multi-factor authentication for all remote network access to privileged and non-privileged accounts for information systems that receive, process, store, or transmit FTI. (CE1, CE2)
c. Implement multi-factor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. NIST SP 800-63 allows the use of software tokens. (CE11)

9.3.7.3 Device Identification and Authentication (IA-3)

The information system must uniquely identify and authenticate devices before establishing a connection.

Organizational devices requiring unique device-to-device identification and authentication may be defined by type, device, or a combination. Information systems typically use of the following to identify and authenticate:

i. Shared known information (e.g., MAC or IP address)
ii. An organizational authentication solution (e.g., IEEE 802.1x and EAP, Radius server, Kerberos).

9.3.7.4 Identifier Management (IA-4)

The agency must manage information system identifiers by:

a. Receiving authorization from designated agency officials to assign an individual, group, role, or device identifier
b. Selecting an identifier that identifies an individual, group, role, or device
c. Assigning the identifier to the intended individual, group, role, or device
d. Preventing reuse of identifiers
e. Disabling the identifier after 120 days

9.3.7.5 Authenticator Management (IA-5)

The agency must manage information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator
b. Establishing initial authenticator content for authenticators defined by the agency
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators

e. Changing default content of authenticators prior to information system installation
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators
g. Changing/refreshing authenticators
h. Protecting authenticator content from unauthorized disclosure and modification

i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators
j. Changing authenticators for group/role accounts when membership to those accounts changes

The information system must, for password-based authentication:

a. Enforce minimum password complexity of:

    1. Eight characters
    2. At least one numeric and at least one special character
    3. A mixture of at least one uppercase and at least one lowercase letter
    4. Storing and transmitting only encrypted representations of passwords
b. Enforce password minimum lifetime restriction of one day
c. Enforce non-privileged account passwords to be changed at least every 90 days
d. Enforce privileged account passwords to be changed at least every 60 days
e. Prohibit password reuse for 24 generations
f. Allow the use of a temporary password for system logon requiring an immediate change to a permanent password
g. Password-protect system initialization (boot) settings

9.3.7.6 Authenticator Feedback (IA-6)

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

9.3.7.7 Cryptographic Module Authentication (IA-7)

The information system must implement mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Validation provides assurance that when agency implements cryptography to protect FTI, the encryption functions have been examined in detail and will operate as intended.

All electronic transmissions of FTI must be encrypted using FIPS 140-2 validated cryptographic modules. A product does not meet the FIPS 140-2 requirements by simply implementing an approved security function. Only modules tested and validated to FIPS 140-2 meet the applicability requirements for cryptographic modules to protect sensitive information. NIST maintains a list of validated cryptographic modules on its website http://csrc.nist.gov/.

9.3.7.8 Identification and Authentication (Non-Organizational Users) (IA-8)

The information system must uniquely identify and authenticate non-agency users (or processes acting on behalf of non-agency users).

9.3.8 Incident Response

These incident response controls apply to both physical and information system security relative to the protection of FTI.

9.3.8.1 Incident Response Policy and Procedures (IR-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls

b. Review and update the current:
    1. Incident response policy every three years
    2. Incident response procedures at least annually

9.3.8.2 Incident Response Training (IR-2)

Agencies must train personnel with access to FTI, including contractors and consolidated data center employees if applicable, in their incident response roles on the information system and FTI. The agency must provide incident response training to information system users consistent with assigned roles and responsibilities:

a. Prior to assuming an incident response role or responsibility
b. When required by information system changes
c. Annually thereafter

9.3.8.3 Incident Response Testing (IR-3)

Agencies entrusted with FTI must test the incident response capability at least annually.

a. Agencies must perform tabletop exercises using scenarios that include a breach of FTI and should test the agency's incident response policies and procedures.
b. A subset of all employees and contractors with access to FTI must be included in table top exercises.
c. Each tabletop exercise must produce an after-action report to improve existing processes, procedures, and policies.

See *Section 10.3, Incident Response Procedures*, for specific instructions on incident response requirements where FTI is involved.

9.3.8.4 Incident Handling (IR-4)

The agency must:

a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery
b. Coordinate incident handling activities with contingency planning activities
c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises
d. implement the resulting changes accordingly

9.3.8.5 Incident Monitoring (IR-5)

The agency must track and document all physical and information system security incidents potentially affecting the confidentiality of FTI.

9.3.8.6 Incident Reporting (IR-6)

The agency must:

a. Require personnel to report suspected security incidents to internal agency incident response resources upon discovery of the incident
b. Contact the appropriate special agent-in-charge, TIGTA, and the IRS Office of Safeguards immediately but no later than 24 hours after identification of a possible issue involving FTI

Refer to *Section 10.0, Reporting Improper Inspections or Disclosures*, for more information on incident reporting requirements required by the Office of Safeguards.

9.3.8.7 Incident Response Assistance (IR-7)

The agency must provide an incident response support resource, integral to the agency incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

9.3.8.8 Incident Response Plan (IR-8)

The agency must:

a. Develop an incident response plan that:
    1. Provides the agency with a roadmap for implementing its incident response capability
    2. Describes the structure of the incident response capability
    3. Provides a high-level approach for how the incident response capability fits into the overall agency

4. Meets the unique requirements of the agency, which relate to mission, size, structure, and functions
5. Defines reportable incidents
6. Provides metrics for measuring the incident response capability within the agency
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability
8. Is reviewed and approved by designated agency officials

b. Distribute copies of the incident response plan to authorized incident response personnel
c. Review the incident response plan at a minimum on an annual basis or as an after-action review
d. Update the incident response plan to address system/agency changes or problems encountered during plan implementation, execution, or testing
e. Communicate incident response plan changes to authorized incident response personnel
f. Protect the incident response plan from unauthorized disclosure and modification

9.3.8.9 Information Spillage Response (IR-9)

The agency must respond to information spills by:

a. Identifying the specific information involved in the information system contamination
b. Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill
c. Isolating the contaminated information system or system component
d. Eradicating the information from the contaminated information system or component
e. Identifying other information systems or system components that may have been subsequently contaminated

9.3.9 Maintenance

9.3.9.1 System Maintenance Policy and Procedures (MA-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance

2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls

b. Review and update the current:

1. System maintenance policy every three years
2. System maintenance procedures at least annually

9.3.9.2 Controlled Maintenance (MA-2)

The agency must:

a. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and agency requirements
c. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location
d. Require that designated agency officials explicitly approve the removal of the information system or system components from agency facilities for off-site maintenance or repairs
e. Sanitize equipment to remove all FTI from associated media prior to removal from agency facilities for off-site maintenance or repairs
f. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions and update agency maintenance records accordingly

9.3.9.3 Maintenance Tools (MA-3)

The agency must approve, control, and monitor information system maintenance tools.

9.3.9.4 Non-Local Maintenance (MA-4)

The agency must:

a. Approve and monitor non-local maintenance and diagnostic activities
b. Allow the use of non-local maintenance and diagnostic tools only as consistent with agency policy and documented in the security plan for the information system
c. Employ multi-factor authenticator in the establishment of non-local maintenance and diagnostic sessions
d. Maintain records for non-local maintenance and diagnostic activities
e. Terminates session and network connections when non-local maintenance is completed
g. Documents policies and procedures for the establishment and use of non-local maintenance and diagnostic connections (CE2)

9.3.9.5 Maintenance Personnel (MA-5)

The agency must:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel
b. Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations
c. Designate agency personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations

9.3.10 Media Protection

Information system media is defined to include both digital and non-digital media.

9.3.10.1 Media Protection Policy and Procedures (MP-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls
b. Review and update the current:
    1. Media protection policy every three years
    2. Media protection procedures at least annually

9.3.10.2 Media Access (MP-2)

The agency must restrict access to digital and non-digital media containing FTI to authorized individuals.

9.3.10.3 Media Marking (MP-3)

The agency must label information system media containing FTI to indicate the distribution limitations and handling caveats.

The agency must label removable media (CDs, DVDs, diskettes, magnetic tapes, external hard drives and flash drives) and information system output containing FTI (reports, documents, data files, back-up tapes) indicating "Federal Tax Information". Notice 129-A and Notice 129-B IRS provided labels can be used for this purpose.

9.3.10.4 Media Storage (MP-4)

The agency must:

a. Physically control and securely store media containing FTI
b. Protect information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures

See *Section 4.0, Secure Storage—IRC 6103(p)(4)(B),* on additional secure storage requirements.

9.3.10.5 Media Transport (MP-5)

The agency must:

a. Protect and control digital (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) and non-digital (e.g., paper) media during transport outside of controlled areas
b. Maintain accountability for information system media during transport outside of controlled areas
b. Document activities associated with the transport of information system media—the agency must use transmittals or an equivalent tracking method to ensure FTI reaches its intended destination
c. Restrict the activities associated with the transport of information system media to authorized personnel

The information system must implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. (CE4)

See *Section 4.4, FTI in Transit*, for more information on transmittals and media transport requirements.

9.3.10.6 Media Sanitization (MP-6)

The agency must:

a. Sanitize media containing FTI prior to disposal, release out of agency control, or release for reuse using IRS-approved sanitization techniques in accordance with applicable federal and agency standards and policies
b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information
c. Review, approve, track, document, and verify media sanitization and disposal actions (CE1)

Agencies must review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Agencies verify that the sanitization of the media was effective prior to disposal (see *Section 9.3.17.9, Information Handling and Retention (SI-12)*).

The agency must restrict the use of information system media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) on information systems that receive, process, store, or transmit FTI using physical or automated controls.

Additional requirements for protecting FTI during media sanitization are provided in *Section 9.3.10.6, Media Sanitization (MP-6)*; *Section 9.4.7, Media Sanitization*; and *Exhibit 10, Data Warehouse Security Requirements*.

9.3.11 Physical and Environmental Protection

9.3.11.1 Physical and Environmental Protection Policy and Procedures (PE-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls
b. Review and update the current:
    1. Physical and environmental protection policy every three years
    2. Physical and environmental protection procedures at least annually

9.3.11.2 Physical Access Authorizations (PE-2)

The agency must:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides
b. Issue authorization credentials for facility access
c. Review the access list detailing authorized facility access by individuals, at least annually
d. Remove individuals from the facility access list when access is no longer required
e. Enforce physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where FTI is received, processed, stored, or transmitted (CE1)

9.3.11.3 Physical Access Control (PE-3)

The agency must:

a. Enforce physical access authorizations at entry/exit points to facilities where the information systems that receive, process, store, or transmit FTI reside by:
    1. Verifying individual access authorizations before granting access to the facility
    2. Controlling ingress/egress to the facility using physical access control systems/devices or guards
b. Maintain physical access audit logs for entry/exit points
c. Provide security safeguards to control access to areas within the facility officially designated as publicly accessible
d. Escort visitors and monitor visitor activity
e. Secure keys, combinations, and other physical access devices
f. Inventory physical access devices
g. Change combinations and keys when an employee who knows the combination retires, terminates employment, or transfers to another position or at least annually

9.3.11.4 Access Control for Transmission Medium (PE-4)

The agency must control physical access within agency facilities.

9.3.11.5 Access Control for Output Devices (PE-5)

The agency must control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Monitors, printers, copiers, scanners, fax machines, and audio devices are examples of information system output devices.

9.3.11.6 Monitoring Physical Access (PE-6)

The agency must:

a. Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents
b. Review physical access logs annually
c. Coordinate results of reviews and investigations with the agency incident response capability
d. Monitor physical intrusion alarms and surveillance equipment (CE1)

9.3.11.7 Visitor Access Records (PE-8)

The agency must:

a. Maintain visitor access records to the facility where the information system resides for 5 years
b. Review visitor access records, at least annually

Also see *Section 4.3, Restricted Area Access*, for visitor access (AAL) requirements.

9.3.11.8 Delivery and Removal (PE-16)

The agency must authorize, monitor, and control information system components entering and exiting the facility and maintain records of those items.

9.3.11.9 Alternate Work Site (PE-17)

The agency must:

a. Employ Office of Safeguards requirements at alternate work sites
b. Assess, as feasible, the effectiveness of security controls at alternate work sites
c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems

> *Alternate work sites may include, for example, government facilities or private residences of employees (*see *Section 4.7, Telework Locations*, for additional requirements).

9.3.11.10 Location of Information System Components (PE-18)

The agency must position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

For additional guidance, see *Section 4.3, Restricted Area Access*, and *Section 4.5, Physical Security of Computers, Electronic, and Removable Media.*

9.3.12 Planning

9.3.12.1 Security Planning Policy and Procedures (PL-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls
b. Review and update the current:
    1. Security planning policy every three years
    2. Security planning procedures at least annually

9.3.12.2 System Security Plan (PL-2)

An approved and accurate SSR satisfies the requirements for the SSP (see *Section 7.0, Reporting Requirements—6103(p)(4)(E)*).

The agency must:

a. Develop an SSR to include information systems that:
    1. Is consistent with the agency's safeguarding requirements
    2. Explicitly defines the information systems that receive, process, store, or transmit FTI
    3. Describes the operational context of the information system in terms of missions and business processes
    4. Describes the operational environment for the information system and relationships with or connections to other information systems
    5. Provides an overview of the security requirements for the system
    6. Identifies any relevant overlays, if applicable
    7. Describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring and supplementation decisions
    8. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation
b. Distribute copies of the SSR and communicate subsequent changes to the SSR to designated agency officials and the Office of Safeguards
c. Review the SSR for the information system on an annual basis

d. Update the SSR to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments
e. Protect the SSR from unauthorized disclosure and modification

9.3.12.3 Rules of Behavior (PL-4)

The agency must:

a. Establish and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage
b. Receive a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system
c. Review and update the rules of behavior at a minimum annually
d. Require individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated
e. Include in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting agency information on public websites—the Office of Safeguards prohibits sharing FTI using any social media/networking sites (CE1)

9.3.13 Personnel Security

(See also *Section 5.1.1 Background Investigation Minimum Requirements*)

9.3.13.1 Personnel Security Policy and Procedures (PS-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:

    1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls

b. Review and update the current:

    1. Personnel security policy every three years
    2. Personnel security procedures at least annually

9.3.13.2 Position Risk Designation (PS-2)
(See also *Section 5.1.1 Background Investigation Minimum Requirements*)

The agency must:

a. Assign a risk designation to all agency positions
b. Establish screening criteria for individuals filling those positions
c. Review and update position risk designations annually
d. Review and update position risk designations annually

9.3.13.3 Personnel Screening (PS-3)
(See also *Section 5.1.1 Background Investigation Minimum Requirements*)

The agency must:

a. Screen individuals prior to authorizing access to the information system
b. Rescreen individuals according to agency-defined conditions requiring rescreening

9.3.13.4 Termination (PS-4)

The agency, upon termination of individual employment must:

a. Disable information system access
b. Terminate/revoke any authenticators/credentials associated with the individual
c. Conduct exit interviews, as needed
d. Retrieve all security-related agency information system–related property
e. Retain access to agency information and information systems formerly controlled by the terminated individual
f. Notify agency personnel upon termination of the employee

9.3.13.5 Personnel Transfer (PS-5)

The agency must:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the agency
b. Initiate transfer or reassignment actions following the formal transfer action
c. Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer
d. Notify designated agency personnel, as required

9.3.13.6 Access Agreements (PS-6)

Before authorizing access to FTI, the agency must:

a. Develop and document access agreements for agency information systems
b. Review and update the access agreements, at least annually
c. Ensure that individuals requiring access to agency information and information systems:
    1. Sign appropriate access agreements prior to being granted access
    2. Re-sign access agreements to maintain access to agency information systems when access agreements have been updated or at least annually

9.3.13.7 Third-Party Personnel Security (PS-7)

The agency must:

a. Establish personnel security requirements, including security roles and responsibilities for third-party providers
b. Require third-party providers to comply with personnel security policies and procedures established by the agency
c. Document personnel security requirements
e. Require third-party providers to notify the agency of any personnel transfers or terminations of third-party personnel who possess agency credentials or badges or who have information system privileges
f. Monitor provider compliance

9.3.13.8 Personnel Sanctions (PS-8)

The agency must:

a. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures
b. Notify designated agency personnel when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction

9.3.14 Risk Assessment

9.3.14.1 Risk Assessment Policy and Procedures (RA-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:

    1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls

b. Review and update the current:

1. Risk assessment policy every three years
2. Risk assessment procedures at least annually

9.3.14.2 Risk Assessment (RA-3)

The agency must:

a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits
b. Document risk assessment results in a risk assessment report
c. Review risk assessment results at least annually
e. Disseminate risk assessment results to designated agency officials
f. Update the risk assessment report at least every three years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system

9.3.14.3 Vulnerability Scanning (RA-5)

The agency must:

a. Scan for vulnerabilities in the information system and hosted applications at a minimum of monthly for all systems and when new vulnerabilities potentially affecting the system/applications are identified and reported
b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations
    2. Formatting checklists and test procedures
    3. Measuring vulnerability impact
c. Analyze vulnerability scan reports and results from security control assessments
d. Remediate legitimate vulnerabilities in accordance with an assessment of risk
e. Share information obtained from the vulnerability scanning process and security control assessments with designated agency officials to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies)
f. Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned (CE1)

9.3.15 System and Services Acquisition

9.3.15.1 System and Services Acquisition Policy and Procedures (SA-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls

b. Review and update the current:

    1. System and services acquisition policy every three years
    2. System and services acquisition procedures at least annually

9.3.15.2 Allocation of Resources (SA-2)

The agency must:

a. Determine information security requirements for the information system or information system service in mission/business process planning
b. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process
c. Establish a discrete line item for information security in agency programming and budgeting documentation

9.3.15.3 System Development Life Cycle (SA-3)

The agency must:

a. Manage the information system using an SDLC that incorporates information security considerations
b. Define and document information security roles and responsibilities throughout the SDLC
c. Identify individuals having information security roles and responsibilities
d. Integrate the agency information security risk management process into SDLC activities

9.3.15.4 Acquisition Process (SA-4)

The agency must include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and agency mission/business needs:

a. Security functional requirements
b. Security strength requirements
c. Security assurance requirements
e. Security-related documentation requirements
f. Requirements for protecting security-related documentation
g. Description of the information system development environment and environment in which the system is intended to operate
h. Acceptance criteria

When applicable, the agency must require the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed (CE1)

9.3.15.5 Information System Documentation (SA-5)

The agency must:

a. Obtain administrator documentation for the information system, system component, or information system service that describes:
    1. Secure configuration, installation, and operation of the system, component, or service
    2. Effective use and maintenance of security functions/mechanisms
    3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions
b. Obtain user documentation for the information system, system component, or information system service that describes:
    1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms
    2. Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner
    3. User responsibilities in maintaining the security of the system, component, or service
c. Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent
d. Protect documentation, as required
e. Distribute documentation to designated agency officials

9.3.15.6 Security Engineering Principles (SA-8)

The agency must apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Security engineering principles include, for example:

(i) developing layered protections
(ii) establishing sound security policy, architecture, and controls as the foundation for design
(iii) incorporating security requirements into the system development lifecycle
(iv) delineating physical and logical security boundaries
(v) ensuring that system developers are trained on how to build secure software
(vi) tailoring security controls to meet organizational and operational needs
(vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk
(viii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

9.3.15.7 External Information System Services (SA-9)

The agency must:

a. Require that providers of external information system services comply with agency information security requirements and employ to include (at a minimum) security requirements contained within this publication and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and established service-level agreements
b. Define and document government oversight and user roles and responsibilities with regard to external information system services
c. Monitor security control compliance by external service providers on an ongoing basis
d. Restrict the location of information systems that receive, process, store, or transmit FTI to areas within the United States territories, embassies, or military installations (CE5)

Agencies must prohibit the use of non-agency-owned information systems, system components, or devices that receive, process, store, or transmit FTI unless explicitly approved by the Office of Safeguards. For notification requirements, refer to Section 7.4.5, Non-Agency-Owned Information Systems.

The contract for the acquisition must contain Exhibit 7 language, as appropriate (see *Section 9.3.15.4, Acquisition Process (SA-4)*, and *Exhibit 7, Safeguarding Contract Language).*

9.3.15.8 Developer Configuration Management (SA-10)

The agency must require the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service development, implementation, and operation
b. Document, manage, and control the integrity of changes to the system, component, or service
c. Implement only agency-approved changes to the system, component, or service
d. Document approved changes to the system, component, or service and the potential security impacts of such changes
b. Track security flaws and flaw resolution within the system, component, or service and report findings to designated agency officials

9.3.15.9 Developer Security Testing and Evaluation (SA-11)

The agency must require the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan
b. Perform security testing/evaluation
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation
d. Implement a verifiable flaw remediation process
e. Correct flaws identified during security testing/evaluation

9.3.15.10 Unsupported System Components (SA-22)

The agency must replace information system components (specifically security patches and/or product updates) when support for the components is no longer available from the developer, vendor, or manufacturer. During a Safeguards on-site review, any unsupported system that is identified will not be tested and will result in a critical finding.

9.3.16 System and Communications Protection

9.3.16.1 System and Communications Protection Policy and Procedures (SC-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls

b. Review and update the current:

    1. System and communications protection policy every three years
    2. System and communications protection procedures at least annually

9.3.16.2 Application Partitioning (SC-2)

The information system must separate user functionality (including user interface services) from information system management functionality.

9.3.16.3 Information in Shared Resources (SC-4)

The information system must prevent unauthorized and unintended information transfer via shared system resources.

9.3.16.4 Denial of Service Protection (SC-5)

The information system must protect against or limit the effects of denial of service attacks.

Refer to *NIST SP 800-61 R2, Computer Security Incident Handling Guide*, for additional information on denial of service.

9.3.16.5 Boundary Protection (SC-7)

The information system must:

a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system
b. Implement subnetworks for publicly accessible system components that are physically and logically separated from internal agency networks
c. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with agency security architecture requirements

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

The agency must limit the number of external network connections to the information system. (CE3)

The agency must: (CE4)

a. Implement a secure managed interface for each external telecommunication service
b. Establish a traffic flow policy for each managed interface
d. Protect the confidentiality and integrity of the information being transmitted across each interface

e. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need, and accept the associated risk
f. Review exceptions to the traffic flow policy at a minimum annually, and remove exceptions that are no longer supported by an explicit mission/business need

The information system at managed interfaces must deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). (CE5)

The information system must, in conjunction with a remote device, prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. (CE7)

Additional requirements for protecting FTI on networks are provided in *Section 9.4.10, Network Protections.*

9.3.16.6 Transmission Confidentiality and Integrity (SC-8)

Information systems that receive, process, store, or transmit FTI, must:

a. Protect the confidentiality and integrity of transmitted information
b. Implement FIPS 140-2 cryptographic mechanisms to prevent unauthorized disclosure of FTI and detect changes to information during transmission across the wide area network (WAN) and within the local area network (LAN) (CE1)

The agency must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized agency personnel. Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic. For physical security protections of transmission medium, see *Section 9.3.11.4, Access Control for Transmission Medium (PE-4).*

This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, fax machines).

9.3.16.7 Network Disconnect (SC-10)

The information system must terminate the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity.

This control addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect) in contrast to user-initiated logical sessions in AC-12.

9.3.16.8 Cryptographic Key Establishment and Management (SC-12)

The agency must establish and manage cryptographic keys for required cryptography employed within the information system.

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures.

9.3.16.9 Cryptographic Protection (SC-13)

The information system must implement cryptographic modules in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

9.3.16.10 Collaborative Computing Devices (SC-15)

The information system must:

a. Prohibit remote activation of collaborative computing devices
b. Provide an explicit indication of use to users physically present at the devices

Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated

9.3.16.11 Public Key Infrastructure Certificates (SC-17)

The agency must issue public key infrastructure certificates or obtain public key infrastructure certificates from an approved service provider.

9.3.16.12 Mobile Code (SC-18)

The agency must:

a. Define acceptable and unacceptable mobile code and mobile code technologies
c. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies
d. Authorize, monitor, and control the use of mobile code within the information system

Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript, which are common installations on most end user workstations. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., tablet computers and smartphones).

9.3.16.13 Voice over Internet Protocol (SC-19)

The agency must:

a. Establish usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously
b. Authorize, monitor, and control the use of VoIP within the information system

Additional requirements for protecting FTI transmitted by VoIP systems are provided in *Section 9.4.15, VoIP Systems*.

9.3.16.14 Session Authenticity (SC-23)

The information system must protect the authenticity of communications sessions. This control addresses communications protection at the session level versus the packet level (e.g., sessions in service-oriented architectures providing Web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

9.3.16.15 Protection of Information at Rest (SC-28)

The information system must protect the confidentiality and integrity of FTI at rest. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

> *Agencies may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms, file share scanning, and integrity protection. Agencies may also employ other security controls, including, for example, secure offline storage in lieu of online storage, when adequate protection of information at rest cannot otherwise be achieved or when continuously monitoring to identify malicious code at rest.*
>
> *The confidentiality and integrity of information at rest shall be protected when located on a secondary (non-mobile) storage device (e.g., disk drive, tape drive) with cryptography mechanisms*

FTI stored on deployed user workstations, in non-volatile storage, shall be encrypted with FIPS-validated or National Security Agency (NSA)-approved encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology.

Mobile devices do require encryption at rest (see *Section 9.3.1.14, Access Control for Mobile Devices (AC-19)*, and *Section 9.4.8, Mobile Devices)*.

9.3.17 System and Information Integrity

9.3.17.1 System and Information Integrity Policy and Procedures (SI-1)

The agency must:

a. Develop, document, and disseminate to designated agency officials:
    1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
    2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls
b. Review and update the current:
    1. System and information integrity policy every three years
    2. System and information integrity procedures at least annually

9.3.17.2 Flaw Remediation (SI-2)

The agency must:

a. Identify, report, and correct information system flaws
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation
c. Install security-relevant software and firmware updates based on severity and associated risk to the confidentiality of FTI
d. Incorporate flaw remediation into the agency configuration management process
e. Centrally manage the flaw remediation process (CE1)

Security-relevant software updates include, for example, patches, service packs, hot fixes, and antivirus signatures.

9.3.17.3 Malicious Code Protection (SI-3)

Malicious code protection includes antivirus software and antimalware and intrusion detection systems.

The agency must:

a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code
b. Update malicious code protection mechanisms whenever new releases are available in accordance with agency configuration management policy and procedures

c. Configure malicious code protection mechanisms to:

    1. Perform periodic scans of the information system weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with agency security policy
    2. Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system
e. Centrally manage malicious code protection mechanisms (CE1)

The information system must automatically update malicious code protection mechanisms. (CE2)

> *Information system entry and exit points include, for example, firewalls, electronic mail servers, Web servers, proxy servers, remote access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files or hidden in files using steganography. Malicious code can be transported by different means, including, for example, Web accesses, electronic mail, electronic mail attachments, and portable storage devices.*

9.3.17.4 Information System Monitoring (SI-4)

The agency must:

a. Monitor the information system to detect:

    1. Attacks and indicators of potential attacks
    2. Unauthorized local, network, and remote connections

b. Identify unauthorized use of the information system
c. Deploy monitoring devices: (i) strategically within the information system to collect agency-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the agency
d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion
e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to agency operations and assets, individuals, other organizations, or the nation, based on law enforcement information, intelligence information, or other credible sources of information
f. Provide information system monitoring information to designated agency officials as needed

g. Analyze outbound communications traffic at the external boundary of the information system and selected interior points within the network (e.g., subnetworks, subsystems) to discover anomalies—anomalies within agency information systems include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses
h. Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications (CE11)
i. Implement host-based monitoring mechanisms (e.g., Host intrusion prevention system (HIPS)) on information systems that receive, process, store, or transmit FTI (CE23)

The information system must:

a. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions (CE4)
b. Alert designated agency officials when indications of compromise or potential compromise occur—alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms; intrusion detection or prevention mechanisms; or boundary protection devices, such as firewalls, gateways, and routers and alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging; agency personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers (CE5)
c. Notify designated agency officials of detected suspicious events and take necessary actions to address suspicious events (CE7)

Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system.

Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software).

Strategic locations for monitoring devices include, for example, selected perimeter locations and nearby server farms supporting critical applications, with such devices typically being employed at the managed interfaces.

9.3.17.5 Security Alerts, Advisories, and Directives (SI-5)

The agency must:

a. Receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis
b. Generate internal security alerts, advisories, and directives as deemed necessary
d. Disseminate security alerts, advisories, and directives to designated agency officials
e. Implement security directives in accordance with established time frames or notify the issuing agency of the degree of noncompliance

9.3.17.6 Spam Protection (SI-8)

The agency must:

a. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages
b. Update spam protection mechanisms when new releases are available in accordance with agency configuration management policy and procedures

9.3.17.7 Information Input Validation (SI-10)

The information system must check the validity of information inputs.

9.3.17.8 Error Handling (SI-11)

The information system must:

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries
b. Reveal error messages only to designated agency officials

9.3.17.9 Information Handling and Retention (SI-12)

The agency must handle and retain information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

9.3.17.10 Memory Protection (SI-16)

The information system must implement safeguards to protect its memory from unauthorized code execution.

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced, with hardware providing the greater strength of mechanism.

9.3.18 Program Management

9.3.18.1 Senior Information Security Officer (PM-2)

The agency must appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an agency-wide information security program.

The security officer described in this control is an agency official. This official is the senior information security officer. Agencies may also refer to this official as the senior information security officer or chief information security officer.

9.4 Additional Computer Security Requirements

9.4.1 Cloud Computing Environments

Background

As defined by NIST, “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.”

While cloud computing offers many potential benefits, it is not without risk. The primary security concerns with cloud computing are:

- Data is not stored in an agency-managed data center
- The agency must rely on the provider’s security controls for protection
- Data is not transferred securely between the cloud provider and service consumer
- Interfaces to access FTI in a cloud environment, including authentication and authorization controls, may not be secured per customer requirements
- Data from multiple customers is potentially commingled in the cloud environment

An agency's cloud implementation is a combination of a service model and a deployment model. Service models consist of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Deployment models consist of private, community, public, and hybrid clouds.

The risk to data varies in each of the four deployment models, with private cloud typically being the lowest risk model and public cloud being the highest risk model. Depending on the deployment model, compensating controls can be accepted in place of the mandatory requirements, but those compensating controls must provide the same level of protection as mandatory controls for safeguarding FTI.

The service and deployment model used in a cloud computing environment will determine the responsibility for security controls implementation between the agency and the cloud provider for the protection of FTI that is stored or processed in the cloud environment. The delineation of security control responsibility is heavily dependent on the service and deployment models of the solution the agency is adopting. For example, if the solution is an SaaS email solution, the agency may be responsible for a small subset of security control responsibilities. If the agency is deploying its own applications to a PaaS or IaaS solution, it will have greater responsibility for securing the application layer and potentially the platform and middleware.

Requirements

The following mandatory controls are applicable for all cloud service and deployment models. However, as stated earlier, depending on the deployment model, compensating controls can be accepted in place of the mandatory requirements provided that those compensating controls afford the same level of protection as mandatory controls for safeguarding FTI. Potential compensating controls will be evaluated by the Office of Safeguards, as part of the cloud computing notification (see first requirement).

To use a cloud computing model to receive, process, store, or transmit FTI, the agency must be in compliance with all requirements in this publication. The following mandatory requirements are in effect for introducing FTI to a cloud environment:

a. Notification Requirement: The agency must notify the Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment
b. Data Isolation: Software, data, and services that receive, process, store, or transmit FTI must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications
c. SLA: The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or SLA with its third-party cloud provider.
d. Data Encryption in Transit: FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate using the FIPS 140-2 compliant module. This requirement must be included in the SLA.

e. Data Encryption at Rest: FTI may need to be encrypted while at rest in the cloud, depending upon the security protocols inherent in the cloud. If the cloud environment cannot appropriately isolate FTI, encryption is a potential compensating control. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant and operate using the FIPS 140-2 compliant module. This requirement must be included in the SLA, if applicable.
f. Persistence of Data in Relieved Assets: Storage devices where FTI has resided must be securely sanitized or destroyed using methods acceptable by NSA and Central Security Service (CSS). This requirement must be included in the SLA.
g. Risk Assessment: The agency must conduct an annual assessment of the security controls in place on all information systems used for receiving, processing, storing, or transmitting FTI. For the annual assessment immediately prior to implementation of the cloud environment and each annual risk assessment (or update to an existing risk assessment) thereafter, the agency must include the cloud environment. The Office of Safeguards will evaluate the risk assessment as part of the notification requirement in Requirement (a.).
h. Security Control Implementation: Customer-defined security controls must be identified, documented, and implemented. The customer-defined security controls, as implemented, must comply with requirements in this publication.

Additional cloud computing security requirements are available on the Office of Safeguards website.

9.4.2 Data Warehouse

The concept of data warehousing consists of a collection of multi-dimensional integrated databases that are used to provide accessible information to clients or end users. The data can be manipulated through different categories or dimensions to facilitate analyzing data in relational databases. The result can provide the client or end user with an enterprise view or snapshot of the information.

Security requirements apply to data warehousing environments, as well as to typical networked environments.

Section 5.2 and Exhibit 10, *Data Warehouse Security Requirements*, provide unique requirements for this environment.

Additional data warehouse security requirements are available on the Office of Safeguards website.

9.4.3 Email Communications

A written policy must be established and distributed which covers the agency's rules concerning email of FTI. If FTI is prohibited from inclusion within emails or email attachments, the policy must clearly state the actions that will be taken if FTI is inadvertently emailed.

If FTI is allowed to be included within emails or email attachments, the agency must only transmit FTI to an authorized recipient and must adhere to the following requirements:

a. Policies and procedures must be implemented to ensure FTI is properly protected and secured when being transmitted via email
c. Mail servers and clients must be securely configured according to the requirements within this publication to protect the confidentially of FTI transmitted in the email system
d. The network infrastructure must be securely configured according to the requirements within this publication to block unauthorized traffic, limit security vulnerabilities, and provide an additional security layer to an agency's mail servers and clients
e. Emails that contain FTI should be properly labeled (e.g., email subject contains "FTI") to ensure that the recipient is aware that the message content contains FTI
f. Audit logging must be implemented to properly track all email that contains FTI
g. Email transmissions that contain FTI must be encrypted using a FIPS 140-2 validated mechanism
h. Malware protection must be implemented at one or more points within the email delivery process to protect against viruses, worms, and other forms of malware

9.4.4 Fax Equipment

A written policy must be established and distributed which covers the agency's rules concerning faxing of FTI. If FTI is prohibited from inclusion within fax communications, the policy must clearly state the actions that will be taken if FTI is inadvertently faxed.

If FTI is allowed to be included within fax communications, the agency must only transmit FTI to an authorized recipient and must adhere to the following requirements:

a. Have a trusted staff member at both the sending and receiving fax machines
b. Accurately maintain broadcast lists and other preset numbers of frequent recipients of FTI
c. Place fax machines in a secured area
d. Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes:

    1. A notification of the sensitivity of the data and the need for protection
    2. A notice to unintended recipients to telephone the sender—collect, if necessary—to report the disclosure and confirm destruction of the information

9.4.5 Integrated Voice Response Systems

To use an Integrated Voice Response (IVR) system that provides FTI over the telephone to a customer, the agency must meet the following requirements:

a. The LAN segment where the IVR system resides is firewalled to prevent direct access from the Internet to the IVR system
b. The operating system and associated software for each system within the architecture that receives, processes, stores, or transmits FTI to an external customer through the IVR is hardened in accordance with the requirements in this publication and is subject to frequent vulnerability testing
c. Independent security testing must be conducted on the IVR system prior to implementation
d. Access to FTI via the IVR system requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two are recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer. Examples of shared secrets include a unique username, PIN number, password, or pass phrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication.

Additional IVR security requirements are available on the Office of Safeguards website.

9.4.6 Live Data Testing

The use of live FTI in test environments should generally be avoided and is not authorized unless specifically approved by the Office of Safeguards through the submission of a Data Testing Request (DTR) form.

The IRS defines *live data* as primarily unmodified, non-sanitized data extracted from taxpayer files that identifies specific individual or corporate taxpayers and includes taxpayer information or tax return information. The use of live data in testing environments is limited to tax administration or other authorized IRS purposes and may be disclosed only to those individuals with a need-to-know.

Any systems within pre-production testing environments ideally will be configured according to requirements in this publication. However the Office of Safeguards understands most agencies may not be able to fully implement all Publication 1075 requirements in a test environment.

Agencies wishing to use live FTI data in pre-production must submit a DTR to the IRS Office of Safeguards for authority to use live data for testing, providing a detailed explanation of the safeguards in place to protect the data and the necessity for using live data during testing.

Need and Use Justification statements should be revised to cover this use of IRS data, if not already addressed. State taxing agencies should check their statements (agreements) to see if “testing purposes” is covered.

Testing efforts that use live FTI data primarily fall into two categories: one-time testing and ongoing testing.

An example of a one-time testing use of live FTI data would be for system testing that is done prior to a new system implementation and, once testing has validated that the data will work properly, the live FTI data is not required to continue to remain in the test environment. For one-time testing efforts, the Office of Safeguards requires the FTI to be deleted from systems and databases upon completion of testing efforts and that the hard drive of the test systems be cleared electronically prior to repurposing the system for other state agency testing efforts.

Duration for ongoing test activities will be agreed upon as part of the live data request process. Some examples of ongoing testing efforts include:

a. Testing of extract, transform, load (ETL) process to validate federal data load to a database
b. Application testing of income modeling that requires data match between the entire population of state and federal returns, where building a set of dummy data is not feasible
c. Testing audit selection queries that run against the entire population of federal returns to identify potential state non-filers, where building a set of dummy data that would correspond to actual state returns is not feasible

9.4.7 Media Sanitization

The type of sanitization performed depends on whether or not the media:

a. Is to be reused by the agency for continued use with FTI?
b. Will be leaving agency control?

If the media will be reused by the agency for the same purpose of storing FTI and will not be leaving organization control, then clearing is a sufficient method of sanitization. If the media will be reused and repurposed for a non-FTI function or will be leaving organization control (i.e., media being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the agency), then purging should be selected as the sanitization method. If the media will not be reused at all, then destroying is the method for media sanitization.

The following media sanitization requirements are required:

a. The requirements are applicable for media used in a “pre-production” or “test” environments
b. The technique for clearing, purging, and destroying media depends on the type of media being sanitized

c. A representative sampling of media must be tested after sanitization has been completed
d. Media sanitization should be witnessed or verified by an agency employee
e. Media sanitization requirements are the same, regardless of where the information system media is located. However, the party responsible for each step of the sanitization process may differ

Additional media sanitization requirements are available on the Office of Safeguards website.

9.4.8 Mobile Devices

Background

Mobile devices (e.g., smartphones, tablets) provide several unique security and management challenges when used to access corporate resources, including sensitive data. Mobile devices can store vast amounts of data and, by default, security options are not enabled. This leaves the devices vulnerable to allowing an unauthorized person to gain access to the information stored on them or accessed through them. In addition, due to the portable nature of mobile devices, they are susceptible to loss or theft. Another challenge to maintaining security of mobile devices is effectively tracking mobile device inventory. Bring your own device (BYOD) presents additional security and privacy challenges, as it may not be possible to fully manage security of personally owned devices; BYOD for access to FTI must, therefore, be restricted to access to e-mail where FTI is encrypted. These unique challenges highlight the need to increase the security posture of mobile devices to ensure the protection of FTI that may be stored on or accessed from a mobile device.

Requirements

To use FTI in a mobile device environment, the agency must meet the following mandatory requirements:

a. Mobile device management controls must be in place that include security policies and procedures, inventory, and standardized security configurations for all devices
b. An annual risk assessment must be conducted of the security controls in place on all devices in the mobile environment used for receiving, processing, storing, or transmitting FTI
c. Protection mechanisms must be in place in case a mobile device is lost or stolen—all data stored on the device must be encrypted, including internal storage and removable media storage, such as Micro Secure Digital (SD) cards
d. All data communication with the agency's internal network must be encrypted using a cryptographic module that is FIPS 140-2 compliant
e. The agency must control end user ability to download only authorized applications to the device and must limit the accessibility to FTI by applications to only authorized applications
f. All mobile device management servers that receive, process, store, or transmit FTI must be hardened in accordance with requirements in this publication

g. A centralized mobile device management solution must be used to authenticate agency-issued and personally owned mobile devices prior to allowing access to the internal network
h. Security events must be logged for all mobile devices and the mobile device management server
i. The agency must disable wireless personal area networks that allow a mobile device to connect to a computer via Bluetooth or near field communication (NFC) for data synchronization and storage
j. Access to hardware, such as the digital camera, global positioning system (GPS), and universal serial bus (USB) interface, must be disabled to the extent possible
k. Disposal of all mobile device component hardware follows media sanitization and disposal procedures (see *Section 9.3.10.6, Media Sanitization (MP-6)*, and *Section 9.4.7, Media Sanitization*).

See *Section 9.3.1.14, Access Control for Mobile Devices (AC-19)*. Additional mobile device security requirements are also available on the Office of Safeguards website.

9.4.9 Multi-Functional Devices and High Volume Printers

To use FTI in a multi-functional device (MFD) or High Volume Printer, the agency must meet the following requirements:

a. The agency should have a current security policy in place for secure configuration and operation of the MFD or High Volume Printer
b. Least functionality controls that must be in place that include disabling all unneeded network protocols, services, and assigning a dedicated static IP address to the MFD or High Volume Printer
c. Strong security controls should be incorporated into the MFD or High Volume Printer management and administration
d. Access enforcement controls must be configured correctly, including access controls for file shares, administrator and non-administrator privileges, and document retention functions
e. MFD's or High Volume Printers should be locked with a mechanism to prevent physical access to the hard disk
f. Firmware should be up to date with the most current firmware available and should be currently supported by the vendor
g. Devices and print spoolers have auditing enabled, including auditing of user access and fax logs (if fax is enabled), and audit logs should be collected and reviewed by a security administrator
h. All FTI data in transit should be encrypted when moving across a WAN and within the LAN
i. Disposal of all hardware follows media sanitization and disposal procedure requirements (see *Section 9.3.10.6, Media Sanitization (MP-6)*, and *Section 9.4.7, Media Sanitization*)

9.4.10 Network Protections

Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems.

Any publicly accessible servers used in the receipt, process, transmission, or storage of FTI must be placed into an enclave.

Network address translation (NAT) must be implemented at the public traffic demarcation point on the network. If NAT is not implemented at the agency's boundary firewall or router, then it must be implemented on each firewall or router that protects network segments that contain infrastructure components which receive, process, store, or transmit FTI.

The agency's managed interfaces employing boundary protection must deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception). All remote traffic must migrate through a managed interface. Firewalls shall be configured to prohibit any transmission control protocol (TCP) or user datagram protocol service or other protocol/service that is not explicitly permitted (i.e., deny by default).

Inbound services shall be prohibited, unless a valid business case can establish their necessity.

See *Section 9.3.16.5, Boundary Protection (SC-7)*. Additional network protection requirements are available on the Office of Safeguards website.

9.4.11 Storage Area Networks

Background

A storage area network (SAN) is a network whose purpose is to transfer data among information systems and the storage elements in high speed. SANs achieve economy of scale by eliminating the need to manage storage from multiple vendors and platforms.

The typical components of a SAN can be broken down into the host layer, the fabric layer, and the storage layer that comprise the networking infrastructure, management devices that organize connection, storage devices/elements, and client computer systems. The storage layer, where FTI resides, comprises physical disk drives, disk arrays, tape libraries, and other storage media.

SAN components that are most vulnerable to attack include connection points between servers, management devices, and IP-based devices. The fundamental issues are that most SAN protocols do not require device authentication and that it is relatively simple to join the SAN fabric with a spoofing and session hijacking technique.

Requirements

To use FTI in a SAN environment, the agency must meet the following mandatory requirements:

a. FTI must be segregated from other agency data within the SAN environment
b. Access controls must be implemented and strictly enforced for all SAN components to limit access to disks containing FTI to authorized users
c. Fibre channel devices must be configured to authenticate other devices with which they communicate in the SAN and authenticate administrator connections
d. FTI must be encrypted while in transit within the SAN environment. SAN management traffic must also be encrypted for SAN components.
e. SAN components must be physically protected in accordance with the minimum protection standards for physical security described in Section 4.0, *Secure Storage—IRC 6103(p)(4)(B).*
f. All components of the SAN that receive, process, store, or transmit FTI must be hardened in accordance with the requirements in this publication (see SAN SCSEM available on the Office of Safeguards website)
g. SAN components must maintain an audit trail, and the agency must review it weekly to track access to FTI in the SAN environment

Additional SAN security requirements are available on the Office of Safeguards website.

9.4.12 System Component Inventory

The agency must maintain a current inventory of information systems that receive, process, store, or transmit FTI in both production and pre-production environments. Updates to the inventory should be a critical step when implementing installations, removals, and updates to the information system. The inventory should accurately reflect and be consistent with the security domain of the current information system to enable the detection of unauthorized access to FTI within production and pre-production environments.

The IRS does not mandate the particular details or a specific format required to capture the inventory of systems with FTI. However, as part of the on-site safeguard review, the IRS will evaluate the agency's inventory to provide a level of assurance that the inventory is comprehensive of all systems that receive, process, store, or transmit FTI in production and pre-production environments.

Additional system component inventory guidance is available on the Office of Safeguards website.

9.4.13 Virtual Desktop Infrastructure

Background

A virtual desktop infrastructure (VDI) provides users access to enterprise resources, including a virtual desktop from locations both internal to and external to the agency's networks. In a VDI environment, a user can access FTI by connecting to a virtual workstation via a vendor-specific agent, connection client, or through an Internet browser from practically any mobile device with Internet access.

This requirement is applicable to VDI environments in which agency-owned and/or non-agency-owned equipment (including personally-owned devices) may be used as the client for the virtual desktop. The agency must demonstrate that despite the ownership and operational location of the client, FTI remains subject to the safeguard requirements and the highest level of attainable security.

Requirements

To use VDI as a means of remote access to FTI and systems that store, transmit, process and/or receive FTI, the agency must meet the following mandatory requirements:

a. VDI components should be segregated so that boundary protections can be implemented and access controls are granulized
b. An access control system must be specifically configured to address the complicated nature of the environment—ensure only authorized clients who conform to agency security policy are permitted access to the VDI
c. Configure the hypervisor, management consoles, and other VDI components using the secure configuration guidelines provided by the vendor
d. The least privilege principle must be strictly enforced in a virtualized environment
e. Configure the virtualized desktop to provide the functionalities only required for operations—non-essential functionality or components must be removed or prohibited
f. Users who access FTI remotely must use multi-factor authentication to validate their identities
g. Privileged and administrative functions must be recorded by the system. Security events must be reviewed regularly by security personnel
h. FTI must be transmitted securely using end-to-end encryption

Additional VDI requirements are available on the Office of Safeguards website.

9.4.14 Virtualization Environments

Background

NIST SP 800-125 defines full virtualization as, “the simulation of the software and/or hardware upon which other software runs.” This simulated environment is called a virtual machine (VM). There are many forms of virtualization, distinguished primarily by computing architecture layer.

Requirements

To use a virtual environment that receives, processes, stores, or transmits FTI, the agency must meet the following mandatory requirements:

a. When FTI is stored in a shared location, the agency must have policies in place to restrict access to FTI to authorized users
b. Programs that control the hypervisor should be secured and restricted to authorized administrators only
c. FTI data transmitted via hypervisor management communication systems on untrusted networks must be encrypted using FIPS-approved methods provided by either the virtualization solution or third-party solution, such as a VPN that encapsulates the management traffic
d. Separation between VMs must be enforced, and functions that allow one VM to share data with the hypervisor or another VM, such as clipboard sharing or shared disks, must be disabled
e. Virtualization providers must be able to monitor for threats and other activity that is occurring within the virtual environment—this includes being able to monitor the movement of FTI into and out of the virtual environment
f. The VMs and hypervisor/host operating system (OS) software for each system within the virtual environment that receives, processes, stores, or transmits FTI must be hardened in accordance with the requirements in this publication and be subject to frequent vulnerability testing
g. Special VM functions available to system administrators in a virtualized environment that can leverage the shared memory space in a virtual environment between the hypervisor and VM should be disabled
h. Virtual systems are configured to prevent FTI from being dumped outside of the VM when system errors occur
i. Vulnerability assessment must be performed on systems in a virtualized environment prior to system implementation
j. Backups (virtual machine snapshot) must be properly secured and must be stored in a logical location where the backup is only accessible to those with a need-to-know

Additional virtualization requirements are available on the Office of Safeguards website.

9.4.15 VoIP Systems

Background

VoIP is the transmission of voice over packet-switched networks. VoIP systems include a variety of components, such as call processors/call managers, gateways, routers, firewalls, and protocols. Data, in the form of a digitized voice conversation, is enclosed in a packet and transported via a data network to a voice gateway that converts voice calls between the IP network and the public switched telephone network. In FTI implementations, this means that telephone conversations between agency personnel and their taxpayer customers where FTI is discussed as part of the conversation are transmitted across the network as a data packet.

Requirements

To use a VoIP network that provides FTI to a customer, the agency must meet the following mandatory requirements:

a. VoIP traffic that contains FTI should be segmented off from non-VoIP
b. When FTI is in transit across the network (either Internet or state agency's network), the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode
c. VoIP network hardware (servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in *Section 4.0, Secure Storage—IRC 6103(p)(4)(B)*
d. Each system within the agency's network that transmits FTI to an external customer through the VoIP network is hardened in accordance with the requirements in this publication and is subject to frequent vulnerability testing
e. VoIP-ready firewalls must be used to filter VoIP traffic on the network
f. Security testing must be conducted on the VoIP system prior to implementation with FTI and annually thereafter
g. VoIP phones must be logically protected, and agencies must be able to track and audit all FTI-applicable conversations and access

Additional VoIP guidance is available on the Office of Safeguards website.

9.4.16 Web-Based Systems

To use an external Web-based system or website (web portal) that provides FTI over the Internet to a customer the agency must meet the following requirements:

a. The system architecture is configured as a three-tier architecture with physically separate systems that provide layered security of the FTI, and access to the database through the application is limited
b. Each system within the architecture that receives, processes, stores, or transmits FTI to an external customer through the Web-based system or website is hardened in accordance with the requirements in this publication and is subject to frequent vulnerability testing

c. Access to FTI via the Web-based system or website requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two is recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer. Examples of shared secrets include a unique username, PIN number, password, or pass phrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication.

9.4.17 Web Browser

Background

The core functions of the Web browser include retrieving information over a network connection (Internet or private network), presenting the information to the users, and sending the information back to the source for a complete transaction. With an increasing amount of information being delivered to the end user via the Web browser, client-side exploits are a growing concern. Web browsers are at the frontline of information security. Most importantly, the default configuration of a Web browser does not provide adequate security. These requirements apply when FTI is accessed through a Web browser.

Requirements

To access FTI using a Web browser, the agency must meet the following mandatory requirements:

a. Install vendor-specified security patches and hot fixes regularly for the Web browser, add-ons, and Java
b. Security enhancements, such as pop-up blocker and content filtering, must be enabled on the Web browser
c. Configure the designated Web browser in accordance to the principle of least functionality and disable items, such as third-party add-ons
d. Deploy a Web gateway to inspect Web traffic and protect the user workstation from direct exposure to the Internet
e. FTI transmission within the agency's internal network must be encrypted using a cryptographic module that is FIPS 140-2 validated
f. Determine the business use of Java and approve the use of Java if is required for core business functions

Additional Web browser security guidance is available on the Office of Safeguards website.

9.4.18 Wireless Networks

Background

A wireless environment is one in which a user can connect to a LAN without physically connecting a device(s) through a wired Ethernet connection. A wireless local area network (WLAN) uses radio waves to broadcast network connectivity to anyone who is within a limited receiving range, such as an office building. WLANs are usually implemented as extensions to existing wired LANs using wireless switches or access points to deliver connectivity to wireless clients, such as laptops or mobile devices. Because of the broadcast and radio nature of wireless technology, ensuring confidentiality is significantly more difficult in a wireless network than a wired network.

These requirements address the security requirements for 802.11 wireless networks that are to be used to receive, process, store, or transmit FTI. This includes wireless networks located at the agency's office or data center from where FTI is received, processed, stored, or transmitted.

Requirements

To use FTI in an 802.11 WLAN, the agency must meet the following mandatory requirements:

a. The agency should have WLAN management controls that include security policies and procedures, a complete inventory of all wireless network components, and standardized security configurations for all components.
b. WLAN hardware (access points, servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in *Section 4.0, Secure Storage—IRC 6103(p)(4)(B).*
c. Each system within the agency's network that transmits FTI through the WLAN is hardened in accordance with the requirements in this publication.
d. The WLAN is architected to provide logical separation between WLANs with different security profiles and from the wired LAN.
e. WLAN infrastructure that receives, processes, stores, or transmits FTI must comply with the Institute of Electrical and Electronic Engineers 802.11i wireless security standard and perform mutual authentication for all access to FTI via 802.1X and extensible authentication protocol
f. Vulnerability scanning should be conducted as part of periodic technical security assessments for the organization's WLAN.
g. Wireless intrusion detection is deployed to monitor for unauthorized access, and security event logging is enabled on WLAN components in accordance with Section 9.3.3, *Audit and Accountability*.
h. Disposal of all WLAN hardware follows media sanitization and disposal procedures in *Section 9.3.10.6, Media Sanitization (MP-6)*, and *Section 9.4.7, Media Sanitization.*

Additional wireless network security requirements are in *Section 9.3.1.13, Wireless Access (AC-18)*, and available on the Office of Safeguards website.

10.0 Reporting Improper Inspections or Disclosures

10.1 General

Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, the individual making the observation or receiving information must contact the office of the appropriate special agent-in-charge, TIGTA immediately, but no later than 24 hours after identification of a possible issue involving FTI. **Call the local TIGTA Field Division Office first**.

Table 11 – TIGTA Field Division Contact Information

Field Division	Field Division Service Locations	Telephone
Atlanta	Alabama, Florida, Georgia, North Carolina, South Carolina, Tennessee, Puerto Rico, and U.S. Virgin Islands	(470) 639-3792
Mid-States	Arkansas, Illinois, Iowa, Kansas, Louisiana, Michigan, Minnesota, Mississippi, Missouri, Nebraska, North Dakota, South Dakota, Wisconsin, Northern Ohio, Oklahoma, Texas, Louisiana, Kansas, Missouri, Nebraska	(713) 209-3711
Denver	Alaska, Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Oregon, Utah, Washington, and Wyoming	(801) 620-7734
New York	Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, and Vermont	(917) 408-5640
San Francisco	California, Hawaii, Guam, American Samoa, Commonwealth of Northern Mariana Islands, Trust Territory of the Pacific Islands	(213) 576-4147
Washington	Delaware, Indiana, Kentucky, Martinsburg Computing Center, Maryland, New Jersey, Pennsylvania, Southern Ohio, Virginia, West Virginia, Washington, DC	(215) 861-1003
Electronic Crimes & Intelligence Division	Any agency reporting a cyber-incident such as data breach may report directly to this division	(240) 613-5230 cybercrimes@tigta.treas.gov

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

Hotline Number: 800-589-3718
TIGTA Homepage: https://www.treasury.gov/tigta
Mailing Address: Treasury Inspector General for Tax Administration
Ben Franklin Station
P.O. Box 589
Washington, DC 20044-0589

10.2 Office of Safeguards Notification Process

Concurrent to notifying TIGTA, the agency must notify the Office of Safeguards by email to Safeguards mailbox, safeguardreports@irs.gov. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including but not limited to:

- Name of agency and agency Point of Contact for resolving data incident with contact information
- Date and time the incident occurred
- Date and time the incident was discovered
- How the incident was discovered
- Description of the incident and the data involved, including specific data elements, if known
- Potential number of FTI records involved; if unknown, provide a range if possible
- Address where the incident occurred
- IT involved (e.g., laptop, server, mainframe)

Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email. Do not include any FTI in the data Incident report.

Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Office of Safeguards as soon as it is available.

The agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

10.3 Incident Response Procedures

The agency must not wait to conduct an internal investigation to determine if FTI was involved in an unauthorized disclosure or data breach. If FTI may have been involved, the agency must contact TIGTA and the IRS immediately.

Incident response policies and procedures required in *Section 9.3.8, Incident Response*, must be used when responding to an identified unauthorized disclosure or data breach incident.

The Office of Safeguards will coordinate with the agency regarding appropriate follow-up actions required to be taken by the agency to ensure continued protection of FTI. Once the incident has been addressed, the agency will conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. Any identified deficiencies in the incident response policies and procedures should be resolved immediately. Additional training on any changes to the incident response policies and procedures should be provided to all employees, including contractors and consolidated data center employees, immediately.

10.4 Incident Response Notification to Impacted Individuals

Notification to impacted individuals regarding an unauthorized disclosure or data breach incident is based upon the agency's internal incident response policy since the FTI is within the agency's possession or control.

However, the agency must inform the Office of Safeguards of notification activities undertaken before release to the impacted individuals. In addition, the agency must inform the Office of Safeguards of any pending media releases, including sharing the text, prior to distribution.

10.5 FTI Suspension, Termination, and Administrative Review

The federal tax regulation 26 CFR 301.6103(p)(7)-1 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. For more information, refer to *Exhibit 3, U.S.C Title 26, CFR 301.6103(p)(7)-1*.

11.0 Disclosure to Other Persons

11.1 General

Disclosure of FTI is prohibited unless authorized by statute. Agencies having access to FTI are not allowed to make further disclosures of that information to their agents or to a contractor unless authorized by statute.

Agencies are encouraged to use specific language in their contractual agreements that clearly state the requirements necessary to protection the confidentiality of FTI and avoid ambivalence or ambiguity. See the model language of Exhibit 7, for additional guidance on appropriate language to be used in the contract, see *Exhibit 6, Contractor 45-Day Notification Procedures*.

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

11.2 Authorized Disclosure Precautions

When disclosure is authorized, the agency must take certain precautions prior to engaging a contractor, namely:

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

Agencies should fully report to the IRS in their SSRs all disclosures of FTI to contractors. Additional disclosures to contractors should be reported on the annual SSR.

Engaging a contractor who may have incidental or inadvertent access to FTI, and will not be performing services which require authorized access to FTI, does not fall under these requirements. An agency may not contract for the disclosure of FTI which is not authorized by IRC 6103. Only contracts for services which require access to FTI to perform their duties under the contract are required to comply with these standards.

11.3 Disclosing FTI to Contractors

The agency must notify the Office of Safeguards prior to re-disclosing FTI to contractors. The agency must notify and obtain written approval from the Office of Safeguards prior to re-disclosing FTI to sub-contractors. (see *Section 7.0, Reporting Requirements—6103(p)(4)(E),* and *Section 7.4, 45-Day Notification Reporting Requirements*, for additional information).

In addition to the notification, the agency must:

a. Establish privacy roles and responsibilities for contractors and service providers
b. Include privacy requirements in contracts and other acquisition-related documents
c. Share FTI externally, only for the authorized purposes identified in the Privacy Act, or described in its notice(s), or in a manner compatible with those purposes
d. Where appropriate, enter into a contract, an SLA, memoranda of understanding, memoranda of agreement, letters of intent, computer matching agreement, or similar agreement, with third parties that specifically describe the FTI covered and specifically enumerate the purposes for which the FTI may be used
e. Monitor, audit, and train its staff on the authorized uses and sharing of FTI with third parties and on the consequences of unauthorized use or sharing of FTI
f. Evaluate any proposed new instances of sharing FTI with third parties to assess whether they are authorized and whether additional or new public notice is required

11.4 Re-Disclosure Agreements

In rare circumstances, under the authority of IRC 6103(p)(2)(B), the IRS may execute and an agreement with an agency which authorizes the re-disclosure of FTI to another entity. These agreements are negotiated and approved by the IRS Headquarters Office of Disclosure with concurrence of the Office of Safeguards.

Federal agencies authorized by statute to enter into re-disclosure agreements are required to provide a copy of the executed agreement to the Office of Safeguards within 30 days of execution. The electronic copy must be sent to the Office of Safeguards via SDT. If SDT is not available, the agreement may be emailed to the SafeguardReports@irs.gov mailbox.

12.0 Return Information in Statistical Reports

12.1 General

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

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

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

12.2 Making a Request under IRC 6103(j)

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

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

12.3 State Tax Agency Statistical Analysis

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

1) Contact the local IRS disclosure manager[‡] and complete a Need and Use Justification for Federal Tax Information Form.
2) The completed and signed form must be returned to the IRS disclosure manager for review and approval. The Office of Safeguards will be notified by the IRS disclosure manager of the request and approval.
3) Changes to the terms of the statistical analysis activities documented in the form must be submitted to the IRS Office of Safeguards as part of the annual SSR (see *Section 2.4, State Tax Agency Limitations*, and *Section 7.2, Safeguard Security Report).*
4) Updates to the form should be made as requested by the IRS disclosure manager.

If the agency requires the use of a contractor to conduct tax modeling, revenue estimation, or other statistical activities, 45-day notification requirements apply (see Section 11.3, Disclosing FTI to Contractors).

12.4 Making a Request under IRC 6108

State agencies seeking statistical information from the IRS must make requests under IRC 6108 and submit the request to the mailing address specified in *Section 12.2, Making a Request under IRC 6103(j).* A charge will be assessed for this service.

[‡] Refer to http://www.irs.gov/uac/IRS-Disclosure-Offices for contact information.

Exhibit 1 USC Title 26, IRC 6103(a) and (b)

IRC SEC. 6103. CONFIDENTIALITY AND DISCLOSURE OF RETURNS AND RETURN INFORMATION

(a) General rule Returns and return information shall be confidential, and except as authorized by this title—

(1) no officer or employee of the United States,

(2) no officer or employee of any State, any local law enforcement agency receiving information under subsection (i)(7)(A), any local child support enforcement agency, or any local agency administering a program listed in subsection (l)(7)(D) who has or had access to returns or return information under this section, and

(3) no other person (or officer or employee thereof) who has or had access to returns or return information under subsection (e)(1)(D)(iii), paragraph (6), (12), (16), (19), (20) or

(4) (21) of subsection (l), paragraph (2) or (4)(B) of subsection (m), or subsection (n), shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions of this section. For purposes of this subsection, the term “officer or employee” includes a former officer or employee.

(b) Definitions For purposes of this section—

(1) Return The term “return” means any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed.

(2) Return information The term “return information” means—

(A) a taxpayer’s identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments, whether the taxpayer’s return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense,

(B) any part of any written determination or any background file document relating to such written determination (as such terms are

defined in section 6110 (b)) which is not open to public inspection under section 6110,

(C) any advance pricing agreement entered into by a taxpayer and the Secretary and any background information related to such agreement or any application for an advance pricing agreement, and

(D) any agreement under section 7121, and any similar agreement, and any background information related to such an agreement or request for such an agreement, but such term does not include data in a form which cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer. Nothing in the preceding sentence, or in any other provision of law, shall be construed to require the disclosure of standards used or to be used for the selection of returns for examination, or data used or to be used for determining such standards, if the Secretary determines that such disclosure will seriously impair assessment, collection, or enforcement under the internal revenue laws.

(3) Taxpayer return information The term “taxpayer return information” means return information as defined in paragraph (2) which is filed with, or furnished to, the Secretary by or on behalf of the taxpayer to whom such return information relates.

(4) Tax administration The term “tax administration”—

(A) means—

(i) the administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws or related statutes (or equivalent laws and statutes of a State) and tax conventions to which the United States is a party, and

(ii) the development and formulation of Federal tax policy relating to existing or proposed internal revenue laws, related statutes, and tax conventions, and

(B) includes assessment, collection, enforcement, litigation, publication, and statistical gathering functions under such laws, statutes, or conventions.

(5) State

(A) In general The term “State” means—

(i) any of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands,

(ii) for purposes of subsections (a)(2), (b)(4), (d)(1), (h)(4), and (p), any municipality—

(I) with a population in excess of 250,000 (as determined under the most recent decennial United States census data available),

(II) which imposes a tax on income or wages, and

(III) with which the Secretary (in his sole discretion) has entered into an agreement regarding disclosure, and

(iii) for purposes of subsections (a)(2), (b)(4), (d)(1), (h)(4), and (p), any governmental entity—

(I) which is formed and operated by a qualified group of municipalities, and

(II) with which the Secretary (in his sole discretion) has entered into an agreement regarding disclosure.

(B) Regional income tax agencies For purposes of subparagraph (A)(iii)—

(i) Qualified group of municipalities The term “qualified group of municipalities” means, with respect to any governmental entity, 2 or more municipalities—

(I) each of which imposes a tax on income or wages,

(II) each of which, under the authority of a State statute, administers the laws relating to the imposition of such taxes through such entity, and

(III) which collectively have a population in excess of 250,000 (as determined under the most recent decennial United States census data available).

(ii) References to State law, etc. For purposes of applying subparagraph (A)(iii) to the subsections referred to in such subparagraph, any reference in such subsections to State law, proceedings, or tax returns shall be treated as references to the law, proceedings, or tax returns, as the case may be, of the municipalities which form and operate the governmental entity referred to in such subparagraph.

(iii) Disclosure to contractors and other agents Notwithstanding any other provision of this section, no return or return information shall be disclosed to any contractor or other agent of a governmental entity referred to in subparagraph (A)(iii) unless such entity, to the satisfaction of the Secretary—

(I) has requirements in effect which require each such contractor or other agent which would have access to returns or return information to provide safeguards (within the meaning of subsection (p)(4)) to protect the confidentiality of such returns or return information,

(II) agrees to conduct an on-site review every 3 years (or a mid-point review in the case of contracts or agreements of less than 3 years in duration) of each contractor or other agent to determine compliance with such requirements,

(III) submits the findings of the most recent review conducted under sub-clause (II) to the Secretary as part of the report required by subsection (p)(4)(E), and

(IV) certifies to the Secretary for the most recent annual period that such contractor or other agent is in compliance with all such requirements. The certification required by sub-clause (IV) shall include the name and address of each contractor and other agent, a description of the contract or agreement with such contractor or other agent, and the duration of such contract or agreement. The requirements of this clause shall not apply to disclosures pursuant to subsection (n) for purposes of Federal tax administration and a rule similar to the rule of subsection (p)(8)(B) shall apply for purposes of this clause.

(6) **Taxpayer identity**

The term “taxpayer identity” means the name of a person with respect to whom a return is filed, his mailing address, his taxpayer identifying number (as described in section 6109), or a combination thereof.

(7) **Inspection**

The terms “inspected” and “inspection” means any examination of a return or return information.

(8) **Disclosure**

The term “disclosure” means providing return or return information known to any person.

(9) **Federal agency**

The term “Federal agency” means an agency within the meaning of section 551 (1) of Title 5, United States Code.

(10) **Chief executive officer**

The term “chief executive officer” means, with respect to any municipality, any elected official and the chief official (even if not elected) of such municipality

(11) **Terrorist incident, threat, or activity**

The term “terrorist incident, threat, or activity” means an incident, threat, or activity involving an act of domestic terrorism (as defined in section 2331 (5) of Title 18, United States Code) or international terrorism (as defined in section 2331(1) of such title).

Exhibit 2 USC Title 26, IRC 6103(p)(4)

Any Federal agency described in subsection (h)(2), (h)(5), (i)(1), (2), (3), (5), or (7), (j)(1), (2), or (5), (k)(8), (l)(1), (2), (3), (5), (10), (11), (13), (14), or (17), or (o)(1), the General Accounting Office, the Congressional Budget Office, or any agency, body, or commission described in subsection (d), (i)(3)(B)(i) or (7)(A)(ii), or (l)(6), (7), (8), (9), (12), (15), or (16) or any other person described in subsection (l)(16), (17), (19), (20) or (21) shall, as a condition for receiving returns or return information—

(A) establish and maintain, to the satisfaction of the Secretary, a permanent system of standardized records with respect to any request, the reason for such request, and the date of such request made by or of it and any disclosure of return or return information made by or to it;

(B) establish and maintain, to the satisfaction of the Secretary, a secure area or place in which such returns or return information shall be stored;

(C) restrict, to the satisfaction of the Secretary, access to the returns or return information only to persons whose duties or responsibilities require access and to whom disclosure may be made under the provisions of this title;

(D) provide such other safeguards which the Secretary determines (and which he prescribes in regulations) to be necessary or appropriate to protect the confidentiality of the returns or return information;

(E) furnish a report to the Secretary, at such time and containing such information as the Secretary may prescribe, which describes the procedures established and utilized by such agency, body, or commission, the General Accounting Office, or the Congressional Budget Office for ensuring the confidentiality of returns and return information required by this paragraph; and

(F) upon completion of use of such returns or return information—

(i) in the case of an agency, body, or commission described in subsection (d), (i)(3)(B)(i), or (l)(6), (7), (8), (9), or (16), or any other person described in subsection (l)(16), (17), (19), or (20) return to the Secretary such returns or return information (along with any copies made therefrom) or make such returns or return information undisclosable in any manner and furnish a written report to the Secretary describing such manner,

(ii) in the case of an agency described in subsections [5] (h)(2), (h)(5), (i)(1), (2), (3), (5) or (7), (j)(1), (2), or (5), (k)(8), (l)(1), (2), (3), (5), (10), (11), (12), (13), (14), (15), or (17), or (o)(1),[6] the General Accounting Office, or the Congressional Budget Office, either—

(I) return to the Secretary such returns or return information (along with any copies made therefrom),

(II) otherwise make such returns or return information undisclosable, or

(III) to the extent not so returned or made undisclosable, ensure that the conditions of subparagraphs (A), (B), (C), (D), and (E) of this paragraph continue to be met with respect to such returns or return information, and

(iii) in the case of the Department of Health and Human Services for purposes of subsection (m)(6), destroy all such return information upon completion of its use in providing the notification for which the information was obtained, so as to make such information undisclosable; except that the conditions of subparagraphs (A), (B), (C), (D), and (E) shall cease to apply with respect to any return or return information if, and to the extent that, such return or return information is disclosed in the course of any judicial or administrative proceeding and made a part of the public record thereof. If the Secretary determines that any such agency, body, or commission, including an agency or any other person described in subsection (l)(16), (17), (19), or (20), or the General Accounting Office or the Congressional Budget Office has failed to, or does not, meet the requirements of this paragraph, he may, after any proceedings for review established under paragraph (7), take such actions as are necessary to ensure such requirements are met, including refusing to disclose returns or return information to such agency, body, or commission, including an agency or any other person described in subsection (l)(16), (17), (19), or (20), or the General Accounting Office or the Congressional Budget Office until he determines that such requirements have been or will be met. In the case of any agency which receives any mailing address under paragraph (2), (4), (6), or (7) of subsection (m) and which discloses any such mailing address to any agent or which receives any information under paragraph (6)(A), (12)(B), or (16) of subsection (l) and which discloses any such information to any agent, or any person including an agent described in subsection (l)(16), this paragraph shall apply to such agency and each such agent or other person (except that, in the case of an agent, or any person including an agent described in subsection (l)(16), any report to the Secretary or other action with respect to the Secretary shall be made or taken through such agency). For purposes of applying this paragraph in any case to which subsection (m)(6) applies, the term “return information” includes related blood donor records (as defined in section 1141(h)(2) of the Social Security Act).

Exhibit 3 USC Title 26, CFR 301.6103(p)(7)-1

USC Title 26, Section 6103(p)(4), requires external agencies and other authorized recipients of federal tax return and return information (FTI) to establish procedures to ensure the adequate protection of the FTI they receive. That provision of the United States Code also authorizes the IRS to take actions, including suspending or terminating FTI disclosures to any external agencies and other authorized recipients, if there is misuse, or if the safeguards in place are inadequate to protect the confidentiality of the information, or both.

Procedures for administrative review of a determination that an authorized recipient has failed to safeguard returns or return information:

(a) *In general.* Notwithstanding any section of the Internal Revenue Code (Code), the Internal Revenue Service (IRS) may terminate or suspend disclosure of returns and return information to any authorized recipient specified in section (p)(4) of section 6103, if the IRS determines that:

  (1) The authorized recipient has allowed an unauthorized inspection or disclosure of returns or return information and that the authorized recipient has not taken adequate corrective action to prevent the recurrence of an unauthorized inspection or disclosure; or
  (2) The authorized recipient does not satisfactorily maintain the safeguards prescribed by section 6103(p)(4), and has made no adequate plan to improve its system to maintain the safeguards satisfactorily.

(b) *Notice of IRS's intention to terminate or suspend disclosure.* Prior to terminating or suspending authorized disclosures, the IRS will notify the authorized recipient in writing of the IRS's preliminary determination and of the IRS's intention to discontinue disclosure of returns and return information to the authorized recipient. Upon so notifying the authorized recipient, the IRS, if it determines that tax administration otherwise would be seriously impaired, may suspend further disclosures of returns and return information to the authorized recipient pending a final determination by the Commissioner or a Deputy Commissioner described in paragraph (d)(2) of this section.

(c) *Authorized recipient's right to appeal.* An authorized recipient shall have 30 days from the date of receipt of a notice described in paragraph (b) of this section to appeal the preliminary determination described in paragraph (b) of this section. The appeal shall be made directly to the Commissioner.

(d) *Procedures for administrative review.*

  (1) To appeal a preliminary determination described in paragraph (b) of this section, the authorized recipient shall send a written request for a conference to: Commissioner of Internal Revenue (Attention: SE:S:CLD:GLD), 1111 Constitution Avenue, NW., Washington, DC 20224. The request must include a complete description of the authorized recipient's present system of safeguarding returns or return information received by the authorized

recipient (and its authorized contractors or agents, if any). The request must state the reason or reasons the authorized recipient believes that such system or practice (including improvements, if any, to such system or practice expected to be made in the near future) is or will be adequate to safeguard returns or return information.

(2) Within 45 days of the receipt of the request made in accordance with the provisions of paragraph (d)(1) of this section, the Commissioner or Deputy Commissioner personally shall hold a conference with representatives of the authorized recipient, after which the Commissioner or Deputy Commissioner shall make a final determination with respect to the appeal.

(e) Effective/applicability date. This section applies to all authorized recipients of returns and return information that are subject to the safeguard requirements set forth in section 6103(p)(4) on or after February 11, 2009.

Exhibit 4 Sanctions for Unauthorized Disclosure

IRC SEC. 7213 UNAUTHORIZED DISCLOSURE OF INFORMATION

(a) RETURNS AND RETURN INFORMATION

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)]. Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) STATE AND OTHER EMPLOYEES—It shall be unlawful for any person [not described in paragraph (1)] willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)] acquired by him or another person under subsection (d), (i)(3)(B)(i), (1)(6), (7), (8), (9), (10), (12), (15) or (16) or (m)(2), (4), (5), (6), or (7) of section 6103. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(3) OTHER PERSONS – It shall be unlawful for any person to whom any return or return information [as defined in section 6103(b)] is disclosed in an manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(4) SOLICITATION – It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information [as defined in 6103(b)] and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(5) SHAREHOLDERS – It shall be unlawful for any person to whom return or return information [as defined in 6103(b)] is disclosed pursuant to the provisions of 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

IRC SEC. 7213A. UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION

(a) PROHIBITIONS

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for

(A) any officer or employee of the United States, or
(B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.

(2) STATE AND OTHER EMPLOYEES – It shall be unlawful for any person [not described in paragraph (l)] willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).

(b) PENALTY

(1) IN GENERAL – Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) FEDERAL OFFICERS OR EMPLOYEES – An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) DEFINITIONS – For purposes of this section, the terms “inspect” “return” and “return information” have respective meanings given such terms by section 6103(b).

Exhibit 5 Civil Damages for Unauthorized Disclosure

IRC SEC. 7431 CIVIL DAMAGES FOR UNAUTHORIZED INSPECTION OR DISCLOSURE OF RETURNS AND RETURN INFORMATION.

(a) In general

(1) Inspection or Disclosure by employee of United States

If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) Inspection or disclosure by a person who is not an employee of United States

If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103 or in violation of section 6104 (c), such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) Exceptions

No liability shall arise under this section with respect to any inspection or disclosure-

(1) which results from good faith, but erroneous, interpretation of section 6103, or
(2) which is requested by the taxpayer.

(c) Damages

In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of –

(1) the greater of –

(A) $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of –

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus

(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the cost of the action.

(d) Period for Bringing Action

Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) Notification of Unlawful Inspection and Disclosure

If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of –

(1) paragraph (1) or (2) of section 7213 (a),

(2) section 7213A (a), or

(3) subparagraph (B) of section 1030(a)(2) of Title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

(f) Definitions

For purposes of this section, the terms “inspect”, “inspection”, “return” and “return information” have the respective meanings given such terms by section 6103 (b).

(g) Extension to information obtained under section 3406

For purposes of this section –

(1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and

(2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in section 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103.

For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 6311 (e).

Exhibit 6 Contractor 45-Day Notification Procedures

Federal agencies, state tax agencies, and state child support enforcement agencies in the possession of FTI may use contractors, sometimes in limited circumstances.

- State tax authorities are authorized by statute to disclose information to contractors for the purpose of, and to the extent necessary in, administering state tax laws, pursuant to Treasury Regulation 301.6103(n)-1.
- Agencies that receive FTI under authority of IRC 6103(l)(7) (human services agencies) may not disclose FTI to contractors for any purpose.

Contractors consist of, but are not limited to, cloud computing providers, consolidated data centers, off-site storage facilities, shred companies, information technology support, or tax modeling or revenue forecasting providers.

Agencies must notify the IRS prior to executing any agreement to disclose FTI to a contractor, or at least 45 days prior to the disclosure of FTI, to ensure that appropriate contractual language is included and that contractors are held to safeguarding requirements. Further, any contractors authorized access to or possession of FTI must notify and secure the approval of the IRS prior to making any redisclosures to subcontractors. For additional information, see *Section 7.4.3, Contractor or Subcontractor Access*.

To provide agency notification of intent to enter into an agreement to make disclosures of FTI to a contractor, submit a letter in electronic format, on agency letterhead over the head of agency's signature, to SafeguardReports@irs.gov. Ensure that the letter contains the following specific information:

- Name, address, phone number, and email address of agency point of contact
- Name and address of contractor
- Contract number and date awarded
- Contract period covered (e.g., 2014–2017)
- Type of service covered by the contract
- Number of contracted workers
- Name and description of agency program that contractor will support
- Detailed description of FTI to be disclosed to contractor
- Description of work to be performed by contractor, including phased timing, how FTI will be accessed, and how tasks may change throughout the different phases
- Procedures for agency oversight on contractor access, storage, and destruction of FTI, disclosure awareness training, and incident reporting
- Location where work will be performed (contractor site or agency location) and how data will be secured if it is moved from the secure agency location
- Statement whether subcontractor(s) will have access to FTI
- Name(s) and address(es) of all subcontractor(s), if applicable
- Description of FTI to be disclosed to subcontractor(s)
- Description of work to be performed by subcontractor(s)

- Location(s) where work will be performed by subcontractor(s) and how data will be secured if it is moved from a secure agency location
- Certification that contractor personnel accessing FTI and contractor information systems containing FTI are all located within the United States or territories, given that FTI is not allowed offshore.

After receipt of an agency's request, the IRS will analyze the information provided to ensure that contractor access is authorized and consistent with all requirements. The IRS will send the agency an email acknowledgement of receipt of agency notification. A written response, along with a reminder of the requirements associated with the contract, is issued once the notification review process is complete. Agency disclosure personnel may wish to discuss local procedures with their procurement colleagues to ensure that they are part of the contract review process and that the appropriate contract language is included from the beginning of the contract.

If the 45-day notification pertains to the use of a contractor to conduct tax modeling, estimate revenue, or employ FTI for other statistical purposes, the agency must also submit a separate statement detailing the methodology and data to be used by the contractor. The Office of Safeguards will forward the methodology and data statement to the IRS Statistics of Income office for approval of the methodology (see Section 7.4.3). Templates can be located on the Office of Safeguards website.

If the 45-day notification is not possible, please contact the Safeguards mailbox at SafeguardReports@irs.gov for assistance.

Exhibit 7 Safeguarding Contract Language

CONTRACT LANGUAGE FOR GENERAL SERVICES

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.

(2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

(3) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.

(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

(5) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

(6) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(7) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(8) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs

of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training provided before the initial certification and

annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

CONTRACT LANGUAGE FOR TECHNOLOGY SERVICES

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the contractor or the contractor's employees.

(2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

(3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(7) All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.

(8) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.

(9) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.(10) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(10) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information,

the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see *Exhibit 4, Sanctions for Unauthorized Disclosure*, and *Exhibit 5, Civil Damages for Unauthorized Disclosure*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Exhibit 8 Warning Banner Examples

A warning banner is required when access is provided to any information system that receives, processes, stores, or transmits FTI. The following elements, as explained in Section 9.3.1.8, *System Use Notification (AC-8)*, must be contained within the warning banner: (i) the system contains U.S. Government information, (ii) user actions are monitored and audited, (iii) unauthorized use of the system is prohibited, and (iv) unauthorized use of the system is subject to criminal and civil sanctions.

The following warning banners are acceptable examples for use by agencies.

WARNING

This system may contain U.S. Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to criminal and civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (the Taxpayer Browsing Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

The following two banners are approved by the Department of Justice for systems that have limited space for the warning banner.

WARNING! BY ACCESSING AND USING THIS GOVERNMENT COMPUTER SYSTEM, YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.

WARNING! THIS SYSTEM CONTAINS U.S. GOVERNMENT INFORMATION. BY ACCESSING AND USING THIS COMPUTER SYSTEM, YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO STATE AND FEDERAL CRIMINAL PROSECUTION AND PENALTIES AS WELL AS CIVIL PENALTIES.

Exhibit 9 Record Retention Schedules

The Office of Safeguards requires the retention of FTI logs only. FTI should be destroyed after use or according to the agency record retention schedule.

Table 12 – Record Retention Schedules

Document Type	Required Document Elements	Retention Schedule
Electronic and Non-Electronic FTI Logs Section 3.2	• Taxpayer name • Tax year(s) • Type of information (e.g., revenue agent reports, Form 1040, work papers) • Reason for request • Date requested • Date received • Exact location of FTI • Person(s) with access to the data, and • Date and method of disposition, if disposed of	5 years
Converted Media Section 3.2	Requirements listed for FTI in its current form (electronic or non-electronic)	5 years
State Auditor Disclosures Section 3.4	Approximate number of records, date of inspection, description of records, name of individual making inspection	5 years
Visitor Access Logs Section 4.3.1	• Name and organization of visitor • Signature of visitor • Form of identification • Date of access • Time of entry and departure • Purpose of visit • Name and organization of person visited	5 years
Disclosure Awareness Certification Section 6.3	Signed disclosure awareness confidentiality statement that certify understanding of FTI security requirements	5 years

Document Type	Required Document Elements	Retention Schedule
Internal Inspections Section 6.4	Internal Inspections • Recordkeeping • Secure storage • Disposal • Limited access • Computer systems security • POA&M	5 years
Audit Trail Logs Section 9.3.3.11	See Section 9.3.3.2, Audit Events (AU-2) See Section 9.3.3.4	7 years

Exhibit 10 Data Warehouse Security Requirements

When an agency implements a data warehouse, the agency must provide written notification to the Office of Safeguards, identifying the security controls, including FTI identification and auditing within the data warehouse. The written notification shall be submitted using SDT or to the SafeguardReports@irs.gov mailbox at least 45 days before implementation. In addition, the agency should update section 9.4.2 Data Warehouse when they submit their annual SSR.

Purpose

The purpose of this document is to provide an overview of data warehousing and data storage concepts and to define the security requirements necessary to protect these environments. Although some security controls may replicate those contained in this publication, such redundancy is necessary so that Exhibit 10 can be used as a stand-alone document. As a rule, all requirements contained within the main text of this publication also apply to any data warehousing environments used by federal, state, or local agencies, and these environments incorporate FTI. These requirements also apply to authorized representatives, agents, or contractors with access to FTI.

This document is intended to describe the controls that are specific to data warehousing-type environments. As the term *data warehousing* is used, the concepts are applied to all complex data environments, including data warehousing, data mining, and data marts.

Audience

This document is intended for federal, state, and local agencies, as well as authorized representatives, agents, or contractors with access to FTI. The document is to be used as a planning document and is intended to support the development and deployment of data warehousing architectures, as well as architectures of a similar environment, such as data marts.

Background

A data warehouse is a structure that is designed to distribute data from multiple arenas to the primary enterprise system. A data mart is a structure designed for access, which is used to facilitate client user support. A data warehouse receives, collects, extracts, transforms, transports, and loads data for a distribution to various data marts.

In the context of FTI within agencies, the data warehouse stores data sets, which contain specific taxpayer information as well as summary information and historical data.

A data warehouse is structured to separate analysis from transaction work and allows a large amount of data to be consolidated from several sources. The security controls remain constant with operational enterprises and are applicable to a data warehouse.

In a data warehouse, the scope of security changes with respect to the different dimensions of data management. Information enters a data warehouse through a staging area where it goes through a process of extraction, transformation, and loading. This process is referred to as ETL. In addition, a data warehouse is operated by query or a search engine tool. Through the use of end-to-end security, the data warehouse ensures the confidentiality, privacy, and integrity of FTI. The security of the data warehouse must include all aspects of the warehouse, including hardware, software, data transport, and data storage.

Data Warehousing Implications

FTI placed in a data warehouse environment may be used only for “tax administration” purposes or for other authorized purposes defined within this publication. As part of the data warehouse, FTI data must retain its identity as FTI to the data element level (i.e., it must be obvious that the IRS is the source of the data). Whenever calculations or data manipulations are performed that could commingle FTI with any other data, the access to FTI must be restricted to agency staff with a need-to-know and their contractors or agents as authorized by law. This requirement is defined in the primary publication but is reinforced here for clarification.

Security

Security controls for data warehousing concepts are derived from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. These controls address the areas of management, operational, and technical controls.

When all controls are implemented and managed, these controls provide effective safeguards for the confidentiality, integrity reliability, and availability of the data. For this document, the defined controls have been mapped to the classes and families of the NIST SP 800-53 to allow technical personnel to easily review NIST controls and understand how these apply to security environments.

The next sections define specific and unique controls related to data warehousing environments. If no additional controls are required, the sections identify this fact.

Management Controls

The following section identifies high-level management controls that shall be used within a data warehousing environment.

Risk Assessment

The agency shall have a risk management program in place to ensure that each aspect of the data warehouse is assessed for risk. Any risk documents shall identify and document all vulnerabilities associated with the data warehousing environment.

Planning

Planning is crucial to the development of a new environment. A security plan shall be in place to address organizational policies, security testing, rules of behavior, contingency plans, architecture and network diagrams, and requirements for security reviews. Although such a security plan will provide planning guidelines, it does not replace requirements documents, which contain specific details and procedures for security operations.

Policies and procedures are required to define how activities and day-to-day procedures will occur. They contain the specific policies, relevant to all of the security disciplines covered in this document. Because they relate to data warehousing, any data warehousing documents can be integrated into overall security procedures. A section shall be dedicated to the data warehouses to define the controls specific to that environment.

The agency must develop policies and procedures to document all existing business processes. The agency must ensure that roles are identified for the organization and develop responsibilities for the roles.

Within the security planning and policies, the purpose or function of the warehouse shall be defined. The business process shall include a detailed definition of configurations and the functions of the hardware and software involved. In general, the planning shall define any unique issues related to data warehousing.

The agency must define how “legacy system data” will be brought into the data warehouse and how the legacy data that is FTI will be cleansed for the ETL transformation process.

The policy shall ensure that FTI will not be subject to public disclosure. Only authorized users with a demonstrated need-to-know can query FTI data within the data warehouse.

System and Services Acquisition

Acquisition security needs to be explored. Because FTI is used within data warehousing environments, it is important that the services and acquisitions have adequate security in place, including the capacity to block information to contractors in cases in which they are not authorized to access FTI.

Certification, Accreditation, and Security Assessments

Certification, accreditation, and security and risk assessments are accepted best practices used to ensure that appropriate levels of control exist, that they are being managed, and that they are compliant with all federal and state laws or statutes.

State and local agencies shall develop a process or policy to ensure that data warehousing security meets the baseline security requirements defined in the current revision of NIST SP 800-53. The process or policy must contain the methodology used

by the state or local agency to inform management, define accountability, and address known security vulnerabilities. Risk assessments must follow the guidelines provided in NIST Publication 800-30, *Risk Management Guide for Information Technology Systems*.

Operational Controls

The following section identifies high-level operational controls that shall be used within a data warehousing environment.

Personnel Security See *Section 5.1.1 Background Investigation Minimum Requirements*

Physical Security and Environmental Protection

There are no additional physical security controls for a data warehousing environment. However, the physical security requirements throughout this publication apply to the physical location that hosts the data warehouse hardware.

Contingency Planning

Online data resources shall be provided adequate tools for the backup, storage, restoration, and validation of data. Agencies will ensure that the data provided is reliable.

Both incremental and special purpose data backup procedures are required, combined with off-site storage protections and regular test-status restoration to validate disaster recovery and business process continuity. Standards and guidelines for these processes are bound by agency policy and are tested and verified. Although already addressed in this publication, the agency's contingency plan must be evaluated to ensure that all data resources are synchronized and restored to allow re-creation of the data to take place.

Configuration Management

The agency shall have a process and documentation to identify and analyze how FTI is used and how FTI is queried or targeted by end users. Parts of the system containing FTI shall be mapped to follow the flow of the query from a client through the authentication server to the release of the query from the database server. During the life cycle of the data warehouse, online and architectural adjustments and changes will occur. The agency shall document these changes and ensure that FTI always is secured from unauthorized access or disclosure.

Maintenance

There are no unique maintenance requirements for data warehousing environments.

System and Information Integrity

There are no unique system and information integrity requirements for data warehousing environments.

Media Protection

The agency shall have policy and procedures in place that describe the cleansing process at the staging area and how the ETL process cleanses the FTI when it is extracted, transformed, and loaded. In addition, the agency shall describe the process of object reuse once FTI is replaced from data sets. IRS requires that all FTI be removed by a random overwrite software program.

Incident Response

Intrusion-detection software shall be installed and maintained to monitor networks for any unauthorized attempt to access tax data. The agency's incident reporting policy and procedures must cover the data warehousing environment as well.

Awareness and Training

The agency shall have a disclosure awareness training program in place that includes how FTI security requirements are communicated to end users. Training shall be user-specific to ensure that all personnel receive appropriate training for a particular job, such as training required for administrators or auditors.

Technical Controls

The following section identifies high-level technical controls that shall be used within a data warehousing environment.

Identification and Authentication

The agency shall configure the Web services to be authenticated before access is granted to users via an authentication server. The Web portal and two-factor authentication requirements in Section 9.0 apply in a data warehouse environment.

Business roles and rules shall be imbedded at either the authentication level or application level. In either case, roles must be in place to ensure that only authorized personnel have access to FTI information.

Authentication shall be required both at the operating system level and at the application level, whenever the data warehousing environment is accessed.

Access Control

Access to systems shall be granted based upon the need to perform job functions. Agencies shall identify which application programs use FTI and how access to FTI is controlled. The access control to application programs relates to how file shares and directories apply file permissions to ensure that only authorized personnel have access to the areas that contain FTI.

The agency shall have security controls in place that include preventive measures to keep an attack from being a success. These security controls shall also include detective measures in place to let the IT staff know that an attack is occurring. If an interruption of service occurs, the agency shall have additional security controls in place that include recovery measures to restore operations.

Within the data warehouse, the agency shall protect FTI as sensitive data and be granted access to FTI for the aspects of its job responsibilities. The agency shall enforce effective access controls so that end users have access to programs with the least privilege needed to complete the job. The agency shall set up access controls in its data warehouse based on personnel clearances. Access controls in a data warehouse are classified in general as follows.

1. General users
2. Limited access users
3. Unlimited access users.

FTI shall always fall into the limited access users category.

All FTI shall have an owner assigned to provide responsibility and accountability for its protection. Typically, this role is assigned to a management official such as an accrediting authority.

The agency shall configure control files and data sets to enable the data owner to analyze and review both authorized and unauthorized accesses.

The database servers that control FTI applications will copy the query request and load it to the remote database to run the application and transform its output to the client. Therefore, access controls must be implemented at the authentication server.

Web-enabled application software shall do the following:

- Prohibit generic meta-characters in input data
- Arrange to have all database queries constructed with parameterized stored procedures to prevent structured query language (SQL) injection
- Protect any variable used in scripts to prevent direct OS command attacks
- Arrange to have all comments removed for any code passed to the browser

- Prevent users from seeing any debugging information on the client
- Undergo a check before production deployment to ensure that all sample, test, and unused files have been removed from the production system.

Audit and Accountability

The agency shall ensure that audit reports are created and reviewed for data warehousing related access attempts.

A data warehouse must capture all changes made to data, including additions, modifications, or deletions by each unique user. If a query is submitted, the audit log must identify the actual query made, the originator of the query, and relevant time and stamp information. For example, if John Doe makes a query to determine the number of people that earn more than $50,000, the audit log would store the fact that John Doe made such a query and its content. The results of the query would not be as significant as the type of query made.

System and Communication Protection

Whenever FTI is located on both production and test environments, these environments are to be segregated. Such action is especially important in the development stages of the data warehouse.

All Internet transmissions are to be encrypted with the use of HTTPS protocol and secure sockets layer encryption based on a certificate that contains a key no less than 128 bits in length, or FIPS 140-2 compliant, whichever is stronger. This encryption will allow information to be protected between the server and the workstation. Data is at its highest risk during the ETL stages when it enters the warehouse. Encryption shall occur as soon as possible. All sessions shall be encrypted and provide end-to-end encryption (i.e., from workstation to point of data).

Web server(s) that receive online transactions shall be configured in a “demilitarized zone” to receive external transmissions but still have some measure of protection against unauthorized intrusion.

Application server(s) and database server(s) shall be configured behind the firewalls for optimal security against unauthorized intrusion. Only authenticated applications and users shall be allowed access to these servers.

Transaction data shall be “swept” from the Web server(s) at frequent intervals, consistent with good system performance, and removed to a secured server behind the firewalls to minimize the risk that these transactions could be destroyed or altered by intrusion.

Antivirus software shall be installed and maintained with current updates on all servers and clients that contain tax data.

For critical online resources, redundant systems shall be employed with automatic failover capability.

Exhibit 11 Media Sanitization Techniques

The technique for clearing, purging, and destroying media depends on the type of media to be sanitized.

Table 13 – Media Sanitization Techniques

Media Type	Clear	Purge	Destroy
Magnetic Disks			
Floppy disks	**Overwrite** media with agency-approved software and validate the overwritten data	**Degauss** with a NSA/CSS- approved degausser	• **Incinerate** floppy disks and diskettes by burning them in a licensed incinerator • **Shred**
ATA hard drives	**Overwrite** media with agency-approved and validated overwriting technologies/methods/ tools	• **Secure erase,** • **Degauss,** or • **Disassemble** and degauss the enclosed platters	• **Incinerate** hard disk drives by burning them in a licensed incinerator • **Shred** • **Pulverize** • **Disintegrate**
USB removable drives	**Overwrite** media with agency-approved and validated overwriting technologies/methods/ tools	• **Secure erase,** • **Degauss** with a NSA/CSS-approved degausser, or **disassemble and degauss** enclosed platters with a NSA/CSS-approved **degausser**	• **Incinerate** hard disk drives by burning them in a licensed incinerator • **Shred** • **Pulverize** • **Disintegrate**
Zip drives	**Overwrite** media with agency-approved and validated overwriting technologies/methods/ tools	**Degauss** with a NSA/CSS-approved degausser	• **Incinerate** disks and diskettes by burning the zip disks in a licensed incinerator • **Shred**
SCSI drives	**Overwrite** media with agency-approved and validated overwriting technologies/methods/ tools	• **Secure erase** • **Degauss** with a NSA/CSS-approved degausser, or • **Disassemble and degauss** the enclosed platters with a NSA/CSS-approved **degausser**	• **Incinerate** hard disk drives by burning them in a licensed incinerator • **Shred** • **Pulverize** • **Disintegrate**

Publication 1075 (Rev. 9-2016) Catalog Number 46937O
Department of the Treasury **Internal Revenue Service** www.irs.gov

(Table 13, Media Sanitization Techniques continued)

Media Type	Clear	Purge	Destroy
Magnetic Tape			
Reel and cassette	**Overwrite** on a system similar to the one originally used to record the data (e.g., overwrite classified or sensitive VHS format video signals on a comparable VHS format recorder); overwrite all portions of the magnetic tape one time with known, nonsensitive signals	**Degauss** with a NSA/CSS-approved degausser	• **Incinerate** by burning the tapes in a licensed incinerator • **Shred**
Optical Disks			
CD/DVDs	N/A; see Destroy method column	N/A; see Destroy method column	Destroy in the following order of recommendations: • Remove the information-bearing layers of DVD media with a commercial optical disk grinding device • Incinerate optical disk media (reduce to ash) with a licensed facility • Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimension of five millimeters and surface area of 25 mm^2.[§]

[§] This particle size is the one currently acceptable. Any disk media shredders obtained in future should reduce CDs and DVDs to a surface area of .25 mm.

A

Accountability: A process of holding users responsible for actions performed on an information system.

Adequate security: Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of information.

Affordable Care Act: U.S. federal statute signed into law on March 23, 2010, with the goal of expanding public and private insurance coverage and reducing the cost of healthcare for individuals and the government.

Alternative work site: Any working area that is attached to the wide area network either through a public switched data network or through the Internet.

Assurance: A measure of confidence that management, operational and technical controls are operating as intended and achieving the security requirements for the system.

Assurance testing: A process used to determine if security features of a system are implemented as designed, and are adequate for the proposed operating environment. This process may include hands-on functional testing, penetration testing, and/or verification.

Audit: An independent examination of security controls associated with a representative subset of organizational information systems to determine the operating effectiveness of system controls; to ensure compliance with established policy and operational procedures; and to recommend changes in controls, policy, or procedures where needed.

Audit trail: A chronological record of system activities sufficient to enable the reconstruction, review, and examination of security events related to an operation, procedure, or event in a transaction from its inception to final results.

Authentication: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system; see *Identification*.

Authorization: Access privileges granted to a user, program, or process.

Availability: Timely, reliable access to information and information services for authorized users.

B

Banner: Display of an information system, which outlines the parameters for system or information use.

Baseline security requirements: A description of the minimum security requirements necessary for an information system to enforce the security policy and maintain an acceptable risk level.

Blurring: The act of obscuring data so that it cannot be read or reconstructed.

C

Classified: National security information classified pursuant to Executive Order 12958.

Compromise: The disclosure of sensitive information to persons not authorized to receive such information.

Comingling: The presence of FTI and non-FTI data together on the same paper or electronic media.

Confidentiality: The preservation of authorized restrictions on information access and disclosure.

Configuration management: A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle.

Container: An object that can be used to hold or transport something.

Containerize: To package (freight) in uniform, sealed containers for shipment.

Control number: A code that identifies a unique document or record.

Control schedule: A record retention and disposal schedule established by the agency.

Corrective Action Plan (CAP): A report required to be filed semi-annually, detailing the agency's planned and completed actions to resolve findings identified during an IRS safeguard review.

Countermeasure: Action, device, procedure, mechanism, technique, or other measure that reduces the vulnerability of an information system.

Cryptography: The process of rendering plain text information unreadable and restoring such unreadable information to a readable form.

D

Data: A representation of facts, concepts, information, or instruction suitable for communication, processing, or interpretation by people or information systems.

Decryption: The process of converting encrypted information into a readable form. This term is also referred to as deciphering.

Degauss: To erase information electromagnetically from a magnetic disk or other storage device.

Digital subscription line: A public telecommunications technology that delivers high bandwidth over conventional copper wire that covers limited distances.

Discretionary access control: A method of restricting logical access to information system objects (e.g., files, directories, devices, permissions, rules) based on the identity and need-to-know of users, groups, or processes.

E

Encryption: See *Cryptography*.

Encryption algorithm: A formula used to convert information into an unreadable format.

Enterprise life cycle: A robust methodology used to implement business change and information technology modernization.

External network: Any network that resides outside the security perimeter established by the telecommunications system.

Extranet: A private data network that uses the public telephone network to establish a secure communications medium among authorized users (e.g., organization, vendors, business partners). An Extranet extends a private network (often referred to as an Intranet) to external parties in cases in which all parties may benefit from the exchange of information quickly and privately.

External information systems: See Non-Agency-Owned Equipment.

Exchange: An online marketplace in which individuals and small businesses can compare policies and buy insurance (with a government subsidy, if eligible).

F

File permission: A method of implementing discretionary access control by establishing and enforcing rules to restrict logical access of information system resources to authorized users and processes.

File server: A local area network computer dedicated to providing files and data storage to other network stations.

Firewall: Telecommunication device used to regulate logical access authorities between network systems.

Firmware: Microcode programming instructions permanently embedded into the read-only memory control block of a computer system. Firmware is a machine component of computer system, similar to a computer circuit component.

G

Gateway: An interface that provides compatibility between heterogeneous networks by converting transmission speeds, protocols, codes, or security rules. This interface is sometimes referred to as a protocol converter.

H

Host: A computer dedicated to providing services to many users. Examples of such systems include mainframes, minicomputers, or servers that provide dynamic host configuration protocol services.

I

Identification: A mechanism used to request access to system resources by providing a recognizable unique form of identification such as a Login ID, User ID, or token; see *Authentication*.

Information: See *Data*.

Information system: A collection of computer hardware, software, firmware, applications, information, communications, and personnel organized to accomplish a specific function or set of functions under direct management control.

Information system security: The protection of information systems and information against unauthorized access, use modification, or disclosure to ensure the confidentiality, integrity, and availability of information systems and information.

Integrity: The protection of information systems and information from unauthorized modification to ensure the quality, accuracy, completeness, nonrepudiation, and authenticity of information.

Internet: Two or more networks connected by a router; the world's largest network, which uses TCP/IP to connect government, university, and commercial institutions.

Intranet: A private network that uses TCP/IP, the Internet, and World Wide Web technologies to share information quickly and privately between authorized user communities, including organizations, vendors, and business partners.

K

Key: Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information.

L

Least privilege: A security principle under which users or processes are assigned the most restrictive set of privileges necessary to perform routine job responsibilities.

M

Management controls: Security controls focused on managing organizational risk and information system security and devising sufficient countermeasures or safeguards to mitigate risk to acceptable levels. Management control families include risk assessment, security planning, system and services acquisition, and security assessment.

Malicious code: Rogue computer programs designed to inflict a magnitude of harm by diminishing the confidentiality, integrity, and availability of information systems and information.

N

Network: A communications infrastructure and all components attached thereto whose primary objective is to transfer information among a collection of interconnected systems. Examples of networks include local area networks, wide area networks, metropolitan area networks, and wireless area networks.

Node: A device or object connected to a network.

Non-Agency-Owned Equipment: Any technology used to receive, process, store, or transmit FTI that is not owned and managed by the agency but is owned by a contractor and centrally managed by their own IT department.

Nonrepudiation: The use of audit trails or secure messaging techniques to ensure the origin and validity of source and destination targets (i.e., senders and recipients of information cannot deny their actions).

O

Object reuse: The reassignment of a storage medium, which contains residual information, to potentially unauthorized users or processes.

Operational controls: Security controls focused on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system, or group of systems. Operational controls require technical or specialized expertise and often rely on management and technical controls. Operational control families include personnel security, contingency planning, configuration management, maintenance, system and information integrity, incident response, and awareness and training.

Organization: An agency or, as appropriate, any of its operational elements.

P

Packet: A unit of information that traverses a network.

Password: A private, protected, alphanumeric string used to authenticate users or processes to information system resources.

Patient Protection and Affordable Care Act: See *Affordable Care Act*.

Penetration testing: A testing method by which security evaluators attempt to circumvent the technical security features of the information system in efforts to identify security vulnerabilities.

Personally identifiable information: Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (e.g., name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual.

Personally-Owned Devices: Any equipment purchased and owned by an individual, not owned by the agency or contractor and not managed by an IT department.

Plan of Action and Milestones (POA&M): A management tool used to assist organizations in identifying, assessing, prioritizing, and monitoring the progress of actions taken to correct security weaknesses found in programs and systems. The POA&M arises from agency-conducted internal inspections and highlights the corrections that result from such inspections (defined in OMB 02-01).

Potential impact: The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect, a serious adverse effect, or a catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Privileged user: A user that has advanced privileges with respect to computer systems. Such users in general include administrators.

Protocol: A set of rules and standards governing the communication process between two or more network entities.

R

Remnants: Residual information remaining on storage media after reallocation or reassignment of such storage media to different organizations, organizational elements, users, or processes. See *Object reuse*.

Residual risk: Portions of risk that remain after security controls or countermeasures are applied.

Risk: The potential adverse impact on the operation of information systems, which is affected by threat occurrences on organizational operations, assets, and people.

Risk assessment: The process of analyzing threats to and vulnerabilities of an information system to determine the potential magnitude of harm, and identify cost-effective countermeasures to mitigate the impact of such threats and vulnerabilities.

Risk management: The identification, assessment, and prioritization of risks.

Router: A device that forwards data packets between computer networks, creating an overlay internetwork.

S

Safeguards: Protective measures prescribed to enforce the security requirements specified for an information system; synonymous with security controls and countermeasures.

Security policy: The set of laws, rules, directives. and practices governing how organizations protect information systems and information.

Security requirement: The description of a specification necessary to enforce the security policy. See *Baseline security requirements*.

Standard user: A general program user, who does not have administrative rights.

Switch: A computer networking device that links network segments or network devices.

System: See *Information system*.

System Security Plan: An official document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements (NIST SP 800-18).

T

Tax modeling: A large-scale microsimulation model of a tax system. Tax models come in all shapes and sizes, depending on the nature of the policy issues examined. The policy questions may relate to specific problems, concerning perhaps the revenue implications of a particular tax, or they may involve an extensive analysis of the cost and redistributive effects of a large number of taxes and transfer payments.

Technical controls: Security controls executed by the computer system through mechanisms contained in the hardware, software, and firmware components of the system. Technical security control families include identification and authentication, access control, audit and accountability, and system and communications protection.

Threat: An activity, event, or circumstance with the potential for causing harm to information system resources.

U

User: A person or process authorized to access an information system.

User identifier: A unique string of characters used by an information system to identify a user or process for authentication.

V

Virus: A self-replicating, malicious program that attaches itself to executable programs.

Voice over Internet Protocol (VoIP): A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet protocol networks, such as the Internet.

Vulnerability: A known deficiency in an information system, which threat agents can exploit to gain unauthorized access to sensitive or classified information.

Vulnerability assessment: Systematic examination of an information system to determine its security posture, identify control deficiencies, propose countermeasures, and validate the operating effectiveness of such security countermeasures after implementation.

Index of Terms

4

45-day Notification, 9, 33, 42, 50, 51, 52, 126, 140

A

access log, 19, 45
Agency Owned, 31
alternative work sites, 24, 25
authentication
  authenticator, 44, 59, 60, 64, 76, 77, 78, 105, 109, 113, 115, 118, 119, 148, 149, 150, 161
Authorized Access List, 20

B

badges, 18, 21, 91

C

Child support, 24
cloud, 51, 68, 105, 106, 107, 139
Cloud Computing, 50, 51, 68, 105
combinations, 18, 22, 86
consolidated data center, 31, 32, 33, 40, 46, 51, 79, 122
Container, 18, 155
contractor, 3, 1, 9, 11, 13, 14, 20, 27, 32, 33, 34, 35, 36, 38, 51, 54, 123, 126, 129, 130, 139, 140, 141, 142, 143, 144, 145, 146
Corrective Action Plan
  CAP, 1, 11, 13, 28, 41, 47, 48, 155
Cryptography, 155, 156

D

data warehouse
  data warehousing, 4, 51, 107, 145, 146, 147, 148, 149, 150, 151
degauss, 152
Degauss, 152, 153, 156
Disclosure Awareness, 4, 37, 38, 39, 63, 143

E

Encryption, 42, 43, 106, 107, 151, 156

F

Fax, 57, 108

H

Human Services, 34, 35, 132

I

incident response, 38, 65, 79, 80, 81, 86, 122, 142, 146, 159
Internal Inspections, 32, 40, 144

K

keys, 18, 22, 86, 99

L

labeling, 29, 44

M

media, 4, 2, 16, 23, 24, 25, 29, 31, 32, 33, 40, 41, 54, 74, 82, 83, 84, 85, 89, 110, 111, 112, 113, 119, 122, 152, 153, 155, 160
Minimum Protection Standards
  MPS, 17, 18, 20
multi-factor, 44, 60, 77, 82, 115

N

need-to-know, 6, 18, 26, 41, 56, 109, 116, 142, 145, 146, 147, 156

O

offshore, 31, 60, 140
off-site, 11, 24, 40, 51, 82, 139, 148

P

password, 25, 43, 45, 64, 78, 109, 118
piggyback, 21
Plan of Action and Milestones
  POA&M, 41, 69, 159

R

Record Retention, 5, 15, 23, 67, 143
recordkeeping, 7, 15, 40, 44
remote access, 59, 60, 77, 102, 115

S

safeguard review, 8, 10, 40, 41, 45, 114, 155
Safeguard Security Report
SSR, 1, 3, 24, 28, 40, 42, 126
Sanitization, 45, 54, 84, 85, 110, 112, 119, 152, 153
Sanitize, 82, 84
SCSEM, 3, 13, 65, 114
SDSEM, 3
subcontractor, 51, 139, 140

T

tailgate, 21
tapes
tape, 19, 23, 29, 40, 41, 54, 83, 84, 85, 153
tax administration, 8, 9, 30, 31, 109, 125, 126, 128, 130, 133, 146
Tax Modeling, 50, 52
TIGTA, 5, 38, 65, 80, 120, 121, 122

V

virus, 25
Visitor, 20, 45, 87, 143
VoIP, 100, 117, 161

W

Warning Banner, 26, 142

Publication 1075 (Rev. 9-2016) Catalog Number 46937O
Department of the Treasury **Internal Revenue Service** www.irs.gov