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 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 Internal Revenue Code (IRC) § 6103(p)(4) safeguard requirements through the identification and mitigation of any risk of loss, breach or misuse of Federal Tax Information (FTI) held by external government agencies.

Office of Safeguards Vision Statement

To serve as a trusted advisor to our Partners, ensuring they have full understanding and insight into FTI requirements and their risk profile, obtain consistent and timely guidance from a "single voice" and receive service and support that is aligned to their risk profile.

We will drive the customer experience and FTI compliance via a collaborative and empowered culture and a cross-trained workforce that is built around a risk-based operating model that integrates infrastructure and processes to enable efficient and effective operations.

Contents

Highlights for November 2021 Revision

This publication revises and supersedes Publication 1075 (November 2016) and is effective 6 months after the publication date. Feedback for Publication 1075 is highly encouraged. Please send any comments to SafeguardReports@irs.gov, using "Publication 1075 comment/feedback" in the subject line. Editorial changes have been made throughout to update references and terms. Web and citation references were added/updated throughout to make the text easier to research in electronic format. Following are the highlighted changes:

1) Publication 1075 has been reformatted, and all sections have been renumbered. Section 1.0 is Federal Tax Information, Reviews and Other Requirements; Section 2.0 is Physical Security Requirements and is numbered to include the applicable IRC § 6103 subsections, the key Safeguarding elements; Section 3.0 is CyberSecurity Requirements; and Section 4.0 is the NIST 800-53 Revision 5 Security and Privacy Controls.

2) Section 4.0, NIST (National Institutes of Standards and Technology) 800-53 Security and Privacy Controls has been updated to align with NIST 800-53 *Revision 5* Security and Privacy controls. Some controls have been added, but all have been reviewed and/or updated.

3) Privacy controls previously in NIST 800-53 Rev 4 Appendix J, are now fully integrated into the NIST controls.

4) NIST SP 800-63, Digital Identity Guidelines, requirements have been adapted into this revision.

5) Treasury Directive 85-01 defined requirements have been included in several Section 4.0 NIST 800-53 Security and Privacy Controls and are shown as *IRS-Defined*.

6) Security and Privacy Control Table has been added for reference. This table identifies the controls, which are privacy related, which overlap with physical controls and identifies those controls new to this revision of the Publication 1075.

7) Many instances of "should" throughout the document have been changed to "must".

8) Key Definitions "Information Spillage", Access, "Unauthorized Inadvertent Access and Incidental Access" have been added. "Unauthorized Disclosure and Need-to-Know have been updated for clarification. The term "Access" was also added.

9) Section 1.2, Authorized Use of FTI has been updated.

10) Section 1.6, Safeguards Reviews now includes the terms "on-site, remote, or a combination of both (hybrid)" as types of assessments and descriptions for on-site reviews and remote reviews.

11) Former Section 2.7, Conducting the Review, has been split into the current Sections 1.6.1, Before the Review, 1.6.2, During the Review and 1.6.3 After the Review, and updated to reflect current on-site review procedures.

12) Former Section 2.7.2, Computer Security Review has been removed and incorporated into Section 3.2 Assessment Process.

13) Former Tables 1 and 2 – Safeguard Review Cycle and IT Testing Techniques have been removed and incorporated into Section 3.2, Assessment Process.

14) Former Section 2.9, Termination of FTI, has been changed to Section 1.7, Termination of FTI-Agency Request.

15) Sections 1.8, Reporting Improper Inspections or Disclosures, 1.9 Disclosures to Other Persons and 1.10 Return Information in Statistical Reports, formerly Sections 10, 11 and 12 have been relocated to the front of Publication 1075.

16) Sections 1.8.1, Terms, 1.8.1.1 Incident and 1.8.1.2 Data Breach are new items.

17) Section 1.8.2, General – Reporting Improper Inspections or Disclosures, was updated to include information regarding spillage and was also updated to reflect the NIST IR Control requirements.

18) Section 1.8.4, Incident Response Procedures now includes requirement for tabletop incident response testing from NIST IR-3 and the requirement to track and document incidents from NIST IR-5.

19) The requirement in former Section 3.1, General Recordkeeping Requirement (now Section 2.A.1), for an inventory of IT systems has been removed. Please see NIST Controls CM-8, System Component Inventory and PM-5, System Inventory, for guidance.

20) Section 2.A.2, Logs of FTI (Electronic and Non-Electronic Receipts), has been updated and references NIST Control AU-2, Audit Events. Additionally, Figure 1 – Sample FTI Logs was updated to include the Electronic Receipts Sample log.

21) Section 2.B.2, Minimum Protection Standards, was updated to include requirements for MFDs or High-Volume Printers.

22) Created new heading for Section 2.B.3.1, Visitor Access Logs and included previous Section 4.2 information.

23) Section 2.B.3.1, Visitor Access Logs, has been updated for clarity and adds retention requirement.

24) Section 2.B.3.2, Authorized Access List has been updated for clarity. The Authorized Access List must be reviewed monthly or upon occurrence or potential indication of an event such as a possible security breach or personnel change.

25) Section 2.B.3.3, Controlling Access to Areas Containing FTI, has been updated for clarity. The agency must maintain a policy addressing issuance of appropriate authorization credentials, including badges, identification cards or smart cards. This policy must include proper use and accountability requirements.

26) Section 2.B.4.1, Security During Office Moves, has been added.

27) Section 2.B.7, Alternate Work Site was formerly Section 4.7, Telework Locations.

28) Section 2.B.7, Alternate Work Site, no longer includes requirement for agency inspections of telework locations

29) Section 2.C.1 General - Restricting Access has been updated to include requirements for auditing controls.

30) Section 2.C.2, Policies and Procedures has been added and includes required policies and procedures related to physical controls. New policies and procedures include Access Control, Audit and Accountability, Media Protection, Privacy Authorization, Physical and Environmental Security, and Personnel Security. Insider Threat Program and Privacy Program plans have also been included.

31) Section 2.C.3, Background Investigation Minimum Requirements has been changed to reflect updated requirement for *reinvestigations to be conducted every five (5) years* (previously 10 years).

32) Section 2.C.3, Background Investigation Minimum Requirements, was rearranged for clarity.

33) Section 2.C.3.1, Background Investigation Requirement Implementation – Removed first paragraph that referenced a one-year implementation period beginning with the last revision of the Publication 1075.

34) Added new Section 2.C.4, Personnel Actions, which includes new Section 2.C.4.1, Personnel Transfer (PS-5), Section 2.C.4.2 Personnel Sanctions (PS-8) and Section 2.C.4.3, Personnel Terminations (PS-4).

35) Added new Section 2.C.7, Offshore Operations, which contains some information that was previously included in former Section 5.3 Access to FTI via State Tax Files or Through Other Agencies.

36) Section 2.C.9, Service Level Agreements (SLA) was formerly Section 5.4.2.2, Consolidated Data Centers and has been updated to reflect more inclusive language, state support functions and includes requirement for Exhibit 7 language.

37) Section 2.D.2.1, Disclosure Awareness Training, has been updated to include the prohibition of FTI in training and a requirement to add role-based training and practical exercises. Training must also include security and privacy updates at least quarterly in addition to annual awareness. The Safeguards' Disclosure Awareness Training video can be used to supplement training but is not intended to fulfill all training requirements.

38) Section 2.D.2.1, Disclosure Awareness Training, has been updated to better align with NIST 800-53 Controls.

39) Section 2.D.2, Table 2, Training Requirements, has been updated to include Insider Threat Awareness Training.

40) Section 2.D.2.2, Disclosure Awareness Training Products, has been updated with current titles of available products.

41) Section 2.D.3, Internal Inspections, has been updated to include self-certification requirements.

42) Section 2.D.9, Plan of Action and Milestones (POA&M) has been updated for clarity.

43) Section 2.E.2 Report Submission Instructions, has been updated to include the Head of Agency may delegate authority to sign Safeguard report submissions.

44) Sections 2.E.4.4, SSR Submission Dates and 2.E.5.2 CAP Submission Dates, have been updated to reflect the correct postal code for CNMI and associated due dates.

45) Previous Section 7.3.1 CAP Submission Instructions and Submission Dates, has been split up into new Sections 2.E.5.1 CAP Submission Instructions and 2.E.5.2, CAP Submission Dates, for clarity.

46) Table 6 in Section 2.E.6, Notification Reporting Requirements has been updated.

47) Section 2.E.6.1 Cloud Computing, and Section 2.E.6.4 Live Data Testing have been updated for

clarity.

48) Removed former Section 7.4.2 Consolidated Data Center.

49) Removed former Section 7.4.4, Data Warehouse Processing.

50) Removed former Section 7.4.5, Non-Agency-owned Information Systems.

51) Removed former Section 7.4.8 Virtualization of Information Technology Systems.

52) Section 2.F.4, Other Precautions, has been updated to reflect *annual* requirement to validate and maintain most recent copy of NAID certification.

53) Former Section 9.4.5, Interactive Voice Response, has been incorporated into Section 3.3.8, Public-Facing Systems (NIST SP 800-63-3).

54) Former Section, 9.4.7, Media Sanitization is now moved to Section 2.F.3.1, under Destruction and Disposal.

55) Former Sections 9.4.11, Storage Area Networks and 9.4.12, System Component Inventory, 9.4.14, Virtualization Requirements, 9.4.15, VoIP Systems and 9.4.18, Wireless Networks, have been removed, as the base requirements are included in NIST controls.

56) Section 3.3.8, Public-Facing Systems, has been added and includes guidance from NIST SP 800-63-3, Digital Identity Guidelines.

57) Former Section 10.5, FTI Suspension, Termination and Administrative Review language was changed and moved to Section 1.7.2.

58) Control IA-2, Identification and Authentication (Organizational Users), Multifactor authentication is now required for all privileged and non-privileged accounts.

59) Exhibit 6, Contractor 45-Day Notification Procedures, has updated the signature requirement to include the Head of Agency, or their delegate.

60) Exhibit 7 has been updated to include Exhibit 7a, Safeguarding Contract Language for General Services and Exhibit 7b, Safeguarding Contract Language for Technology Services.

61) Exhibits 7a and 7b have been updated to include Data Incident Response language.

62) Exhibit 10, Data Warehouse Security Requirements has been removed. Please see the Safeguards Website for technical guidance.

63) Exhibit 11, Media Sanitization Techniques has been removed. Please see NIST 800-88, Guidelines for Media Sanitization for approved sanitization techniques. Also see MP-6.

64) Glossary and Key Terms has been updated to include the terms Access, Contractor, External Systems, Inadvertent and Incidental Access, Information Spillage, Insider Threat, Mobile Code, Mobile Device, Need-to-Know, Object, Remote Access, Subject, Unauthorized Access and Unauthorized Disclosure.

65) Glossary and Key Terms - The definition for Personally Identifiable Information (PII) has been updated to clarify that for the purposes of Publication 1075 and Safeguarding requirements, PII is FTI.

66) Agencies must wipe mobile devices after 10 (ten) unsuccessful login attempts. See AC-7, CE-2.

67) Agencies must employ data mining prevention and detection techniques. See AC-23.

68) Added penetration testing requirements. See CA-8.

69) Perform security and privacy compliance checks prior to allowing connections. See CA-9, CE-1.

70) Multi-factor authentication is required to be at Authenticator Assurance Level 2 as defined in NIST SP 800-63. See IA-2, CE-6.

71) Password complexity requirements have been updated. See IA-5.

72) Agencies must provide training specific training for incidents related to breaches. See IR-2, CE-3.

73) Coordination with contractors, data centers, counties, and other agencies is required for incidents involving Federal Tax Information. See IR-4, CE-8.

74) A custodian must be identified when transporting controls outside of controlled areas. See MP-5, CE-3.

75) Major change to PE-6. The requirement moved from annually to monthly for inspection of physical access logs.

76) Perimeter security checks are required daily for exfiltration of information. See PE-3, CE-2.

77) New Control Enhancement for Defense in Depth. See PL-8, CE-1.

78) Agency contractors (including sub-contractors) must remove data within 7 (seven) calendar days of contract termination. See SA-4, CE-12.

79) Control Enhancement to restrict the accessing, processing, storage, and transmission of FTI to the United States and its territories. See SA-9, CE-5.

80) Change from specifying FIPS 140-3 to latest FIPS validated mechanisms. See SC-13.

81) Added visibility of encrypted communications to system monitoring requirements. See SI-4, CE-10.

Security and Privacy Control Table

Control Number	Control Name	Control Enhancements	Privacy-Related	Physical	Information Technology	Physical Security Reference Section
AC-1	Access Control Policy and Procedures				X	
AC-2	Account Management	X			X	
AC-3	Access Enforcement	X			X	
AC-4	Information Flow Enforcement				X	
AC-5	Separation of Duties				X	
AC-6	Least Privilege	X		X	X	Need-to-Know
AC-7	Unsuccessful Logon Attempts	X			X	
AC-8	System Use Notification			X	X	Exhibit 8
AC-11	Device Lock	X			X	
AC-12	Session Termination				X	
AC-14	Permitted Actions Without Identification or Authentication				X	
AC-17	Remote Access	X		X	X	2.B.7
AC-18	Wireless Access	X			X	
AC-19	Access Control for Mobile Devices	X			X	
AC-20	Use of External Systems	X		X	X	2.B.7.1
AC-21	Information Sharing		X	X	X	Exhibit 7
AC-22	Publicly Accessible Content			X	X	3.3.8
AC-23	Data Mining Protection*				X	
AT-1	Awareness and Training Policy and Procedures		X	X	X	2.C.2
AT-2	Awareness Training	X	X	X	X	2.D.2.1
AT-3	Role-Based Training	X	X	X	X	2.D.2.1
AT-4	Training Records		X	X	X	2.D.2.1
AT-6	Training Feedback*				X	
AU-1	Audit and Accountability Policy and Procedures			X	X	2.C.2
AU-2	Audit Events	X		X	X	2.C.1
AU-3	Content of Audit Records	X			X	
AU-4	Audit Storage Capacity				X	
AU-5	Response to Audit Processing Failures				X	
AU-6	Audit Review, Analysis and Reporting	X		X	X	2.C.1
AU-7	Audit Reduction and Report Generation	X		X	X	2.C.1
AU-8	Time Stamps	X			X	
AU-9	Protection of Audit	X			X	

Control Number	Control Name	Control Enhancements	Privacy-Related	Physical	Information Technology	Physical Security Reference Section
AU-11	Audit Record Retention		X		X	
AU-12	Audit Generation			X	X	2.C.1
AU-16	Cross-Organizational Auditing*		X		X	
CA-1	Assessment, Authorization and Monitoring Policy and Procedures		X		X	
CA-2	Assessments	X	X		X	
CA-3	System Interconnections	X			X	
CA-5	Plan of Action and Milestones		X	X	X	2.D.9
CA-6	Authorization				X	
CA-7	Continuous Monitoring	X	X	X	X	2.D.3
CA-8	Penetration Testing				X	
CA-9	Internal System Connections*	X			X	
CM-1	Configuration Management Policy and Procedures		X		X	
CM-2	Baseline Configuration	X			X	
CM-3	Configuration Change Control	X			X	
CM-4	Security and Privacy Impact Analyses	X	X		X	
CM-5	Access Restrictions for Change	X		X	X	2.C.1
CM-6	Configuration Settings				X	
CM-7	Least Functionality	X			X	
CM-8	System Component Inventory	X			X	
CM-9	Configuration Management Plan				X	
CM-10	Software Usage Restrictions				X	
CM-11	User-Installed Software	X			X	
CM-12	Information Location*	X	X	X	X	3.2
CM-13	Data Action Mapping*				X	
CM-14	Signed Components*				X	
CP-1	Contingency Planning Policy and Procedures		X		X	
CP-2	Contingency Plan	X	X		X	
CP-3	Contingency Training		X		X	
CP-4	Contingency Plan Testing	X	X		X	
CP-9	System Backup	X		X	X	2.B.6
CP-10	System Recovery and Reconstitution	X			X	
IA-1	Identification and Authentication Policy and Procedures		X		X	
IA-2	Identification and Authentication (Organizational Users)	X			X	
IA-3	Device Identification and Authentication				X	

Control Number	Control Name	Control Enhancements	Privacy-Related	Physical	Information Technology	Physical Security Reference Section
IA-4	Identifier Management	X	X		X	
IA-5	Authenticator Management	X			X	
IA-6	Authenticator Feedback				X	
IA-7	Cryptographic Module Authentication				X	
IA-8	Identification and Authentication (Non-Organizational Users)	X			X	
IA-9	Service Identification and Authentication*				X	
IA-11	Re-Authentication*				X	
IA-12	Identity Proofing*	X			X	
IR-1	Incident Response Policy and Procedures		X	X	X	2.C.2
IR-2	Incident Response Training	X	X	X	X	2.D.2.1
IR-3	Incident Response Testing	X	X	X	X	1.8.4
IR-4	Incident Handling	X	X	X	X	1.8.4
IR-5	Incident Monitoring	X	X	X	X	1.8.4
IR-6	Incident Reporting	X	X	X	X	1.8.2
IR-7	Incident Response Assistance	X	X		X	
IR-8	Incident Response Plan		X	X	X	1.8.2
IR-9	Information Spillage Response	X			X	
MA-1	System Maintenance Policy and Procedures				X	
MA-2	Controlled Maintenance	X		X	X	2.B.3.2
MA-3	Maintenance Tools	X			X	
MA-4	Nonlocal Maintenance	X			X	
MA-5	Maintenance Personnel	X		X		2.B.3.3
MA-6	Timely Maintenance*				X	
MP-1	Media Protection Policy and Procedures			X		2.C.2
MP-2	Media Access			X		2.C.11
MP-3	Media Marking			X		2.B.6
MP-4	Media Storage			X		2.B.6
MP-5	Media Transport	X		X		2.B.4
MP-6	Media Sanitization	X		X		2.F.3.1
MP-7	Media Use*	X		X	X	2.B.7.1
PE-1	Physical and Environmental Policy and Procedures			X		2.C.2
PE-2	Physical Access Authorizations			X		2.B.3.2
PE-3	Physical Access Control	X		X		2.B.3
PE-4	Access Control for Transmission			X		2.B.2
PE-5	Access Control for Output			X		2.B.3.3

Control Number	Control Name	Control Enhancements	Privacy-Related	Physical	Information Technology	Physical Security Reference Section
	Devices					
PE-6	Monitoring Physical Access	X		X		2.B.3.2
PE-8	Visitor Access Records			X		2.B.3.1
PE-16	Delivery and Removal			X		2.B.4
PE-17	Alternate Work Site			X		2.B.7
PL-1	Planning Policy and Procedures		X		X	
PL-2	Security and Privacy Plans		X	X	X	2.E.4
PL-4	Rules of Behavior	X	X		X	
PL-8	Security and Privacy Architectures	X	X		X	
PM-1	Information Security Program Plan*				X	
PM-2	Information Security Program Roles				X	
PM-3	Information Security and Privacy Resources*		X		X	
PM-4	Plan of Action and Milestones Process*		X	X	X	2.D.9
PM-5	System Inventory*	X			X	
PM-7	Enterprise Architecture*	X	X		X	
PM-9	Risk Management Strategy*		X		X	
PM-10	Authorization Process		X		X	
PM-12	Insider Threat Program*			X	X	2.C.2
PM-14	Testing, Training and Monitoring*		X	X	X	2.D.2
PM-18	Privacy Program Plan*		X	X	X	2.C.2
PM-19	Privacy Program Roles*		X	X	X	2.C.2
PM-21	Accounting of Disclosures*		X		X	
PM-29	Risk Management Program Leadership Roles*				X	
PS-1	Personnel Security Policy and Procedures			X		2.C.2
PS-2	Position Risk Designation			X		2.C.2
PS-3	Personnel Screening			X		2.C.2
PS-4	Personnel Termination			X		2.C.4.3
PS-5	Personnel Transfer			X		2.C.4.1
PS-6	Access Agreements	X		X		2.C.2
PS-7	External Personnel Security			X		1.9.3
PS-8	Personnel Sanctions			X		2.C.4.2
PS-9	Position Descriptions*			X		
PT-1	Personally Identifiable Information Processing and Transparency Policy and Procedures*		X			

Control Number	Control Name	Control Enhancements	Privacy-Related	Physical	Information Technology	Physical Security Reference Section
PT-2	Authority to Process Personally Identifiable Information*		X			
RA-1	Risk Assessment Policy and Procedures		X		X	
RA-3	Risk Assessment	X	X		X	
RA-5	Vulnerability Scanning	X			X	
RA-7	Risk Response*		X		X	
RA-8	Privacy Impact Assessments*		X	X	X	2.E.4.1
SA-1	System and Services Acquisition Policy and Procedures		X		X	
SA-2	Allocation of Resources				X	
SA-3	System Development Life Cycle	X	X		X	
SA-4	Acquisition Process	X	X	X	X	2.C.7
SA-5	Information System Documentation				X	
SA-8	Security Engineering Principles		X		X	
SA-9	External System Services	X	X		X	
SA-10	Developer Configuration Management	X			X	
SA-11	Developer Security Testing and Evaluation	X	X		X	
SA-15	Development Process, Standards and Tools*	X			X	
SA-22	Unsupported System Components				X	
SC-1	System and Communications Protection Policy and Procedures		X		X	
SC-2	Application Partitioning	X			X	
SC-4	Information in Shared System Resources				X	
SC-7	Boundary Protection	X			X	
SC-8	Transmission Confidentiality and Integrity	X			X	
SC-10	Network Disconnect				X	
SC-12	Cryptographic Key Establishment and Management	X			X	
SC-13	Cryptographic Protection				X	
SC-15	Collaborative Computing Devices and Applications				X	
SC-17	Public Key Infrastructure Certificates				X	
SC-18	Mobile Code	X			X	

Control Number	Control Name	Control Enhancements	Privacy-Related	Physical	Information Technology	Physical Security Reference Section
SC-20	Secure Name/Address Resolution Service (Authoritative Source)*	X			X	
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)*				X	
SC-22	Architecture and Provisioning for Name/Address Resolution Service*				X	
SC-23	Session Authenticity	X			X	
SC-28	Protection of Information at Rest	X			X	
SC-35	External Malicious Code Identification*				X	
SC-39	Process Isolation*				X	
SC-45	System Time Synchronization*	X			X	
SI-1	System and Information Integrity Policy and Procedures		X		X	
SI-2	Flaw Remediation	X			X	
SI-3	Malicious Code Protection	X			X	
SI-4	System Monitoring	X			X	
SI-5	Security Alerts, Advisories and Directives				X	
SI-7	Software, Firmware and Information Integrity*	X			X	
SI-8	Spam Protection	X			X	
SI-10	Information Input Validation				X	
SI-11	Error Handling				X	
SI-12	Information Management and Retention*	X	X		X	
SI-16	Memory Protection				X	
SR-1	Policy and Procedures				X	
SR-2	Supply Chain Risk Management Plan	X			X	
SR-3	Supply Chain Controls and Processes	X			X	
SR-6	Supplier Assessments and Reviews				X	
SR-10	Inspection of Systems or Components				X	
SR-11	Component Authenticity	X			X	

*New to this revision of Publication 1075

INTRODUCTION

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 (FTI). Additionally, IRC § 7213A makes the unauthorized inspection of FTI a misdemeanor, punishable by fines, imprisonment, or both. And finally, IRC § 7431 prescribes civil damages available to the taxpayer upon notification that a criminal indictment or the existence of information that an unauthorized inspection or disclosure has occurred under IRC §§ 7213 or 7213(A).

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

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 or sub-contractor services, it becomes equally important that contractors or sub-contractors protect that information from unauthorized use, access, and disclosure.

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

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

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

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.

Overview of Publication 1075

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

Enterprise security policies address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance to implement all applicable security controls. 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, contractors, and sub-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.

IRS 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 Safeguards and posted on the Safeguards website.

SAFEGUARD RESOURCES

Safeguards Website

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.

The website contains many resources to assist agencies with meeting Publication 1075 requirements. Examples of the website's features include:

- Safeguard alerts and technical assistance documents
- Recommendations on how to comply with Publication 1075 requirements
- Reporting requirement templates (e.g., SSR) and guidance
- Instructions for reporting unauthorized accesses, disclosures, or data breaches
- Internal inspections report templates and instructions

- IRS disclosure awareness videos and resources
- Review Preparation Questionnaire (RPQ)
- Cybersecurity requirements documented in Safeguard Computer Security Evaluation Matrix (SCSEM) templates organized by technology or topic
- Nessus audit files

Safeguards Mailbox

The Safeguards Mailbox is an acceptable alternative for communicating information or questions to the Office of Safeguards relative to safeguarding requirements and Publication 1075. The Mailbox is located at SafeguardReports@irs.gov. The Office of Safeguards requires that all reports, when sent to the Office of Safeguards via email, be transmitted using IRS-approved encryption methods as described in Section 2.E.3 Encryption Requirements. 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
- Data Incident Reporting
- Ad hoc Points of Contact changes

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.

Federal Tax Information

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

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

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

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

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.[1] Forms include supporting schedules, attachments or lists that are supplemental to or part of such a return.

Return information, in general, is any information collected or generated by the IRS regarding 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

Personally Identifiable Information (PII)

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
- Email addresses
- Telephone numbers
- Social Security Numbers
- Bank account numbers
- Date and place of birth
- Mother's maiden name

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

- Biometric data (e.g., height, weight, eye color, fingerprints)
- Any combination of the above

For the purposes of Publication 1075 and Safeguarding requirements, PII is FTI when provided by the IRS or a secondary source (i.e., SSA, BFS).

Information Received from Taxpayers or Third Parties

Copies of tax returns or return information provided to the agency directly by the taxpayer or their 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 (i.e., SSA, BFS) with the taxpayer or a third-party source (linked to the taxpayer), the verified information is no longer FTI as long as the IRS source information is replaced or overwritten with the newly provided information.

Access

Access means when an individual: (1) enters a restricted or locked area, room, container, or system containing federal tax information; or (2) obtains, acquires, receives, examines, uses, or gains knowledge of federal tax information, by physical, electronic, or any other methods.

Users (e.g., system administrators, database administrators) have access to FTI if they have the ability to modify or bypass security controls protecting FTI (to include decryption keys).

Cloud Computing

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.

Inadvertent Access

Access to FTI without authority that is non-willful and unanticipated or accidental.

Inadvertent Disclosure

Accidental exposure of information to a person not authorized access.

Incidental Access

Access to FTI without a need-to-know that may occur in extraordinary circumstances (i.e., system failure, data incident response, disaster response).

Unauthorized Access

Unauthorized access occurs when a person gains logical or physical access to FTI without authority under IRC § 6103 and without a need-to-know (which would include but is not limited to agency employees with no need to know and/or janitors and security guards when there is no second barrier securing the federal tax information as well as developers/administrators of electronic systems/applications receiving, processing, storing or transmitting federal tax information).

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. Inadvertent access is access to FTI without authority and is non-willful. Willful access to FTI by a person without authorization or need-to-know may be prosecuted under IRC § 7213A.

Unauthorized Disclosure

Unauthorized disclosure occurs when a person with access to FTI discloses it to another person without authority under IRC § 6103.

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. Inadvertent disclosure is disclosure of FTI without authority and is non-willful. Willful disclosure of FTI to a person without authorization or need-to-know may be prosecuted under IRC § 7213.

Need-to-Know

Need-to-know is established when individuals require FTI to perform their official duties and are authorized under the IRC.

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. FTI disclosures must be limited to what is essential to accomplish official duties.

Adverse Action

An adverse action includes a suspension of 15 days or more, a reduction in pay, or termination of employment.

Disciplinary Action

A disciplinary action includes an admonishment, written reprimand, or suspension of 14 days or less.

Personnel Sanction

A disciplinary or adverse action for individuals failing to comply with established information security policies and procedures constitutes a personnel sanction.

1.0 FEDERAL TAX INFORMATION, REVIEWS and OTHER REQUIREMENTS

1.1 General

IRC § 6103 is a confidentiality statute and generally prohibits the disclosure of FTI (see Exhibit 1, IRC § 6103(a) and (b), 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 (5) 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 a SSR to Safeguards at least 90 days before the scheduled or requested receipt of FTI (see Section 2.E, Reporting Requirements—6103(p)(4)(E)). The SSR must include processing and safeguard procedures for all FTI received and distinguish between agency programs and functional organizations using FTI. Multiple organizations, divisions or programs within a federal agency using FTI must be consolidated into a single report for that agency at the direction of Safeguards.

Agencies entering into an agreement to disclose FTI to agents, contractors, or sub-contractors requires advance notice to IRS Safeguards (see Section 2.E.6 Notification Reporting Requirements and Section 1.9.4, Disclosing FTI to Contractors or Sub-Contractors.)

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.

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

1.3 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.

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.

1.4 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 Statement for Use of Federal Tax Information form and follow the established guidelines (available through the assigned Governmental Liaison).

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

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

If the agency intends to use a contractor or sub-contractor for conducting statistical analysis, tax modeling or revenue projections, it must submit a 45-day notification (see Section 1.9.4, Disclosing FTI to Contractors or Sub-Contractors) prior to contractor or sub-contractor access to the FTI. The agency'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 or sub-contractor. The Office of Safeguards and Statistics of Income functions will review the information provided to confirm that

adequate safeguarding protocols are in place and that the modeling methodology to be used to remove taxpayer identifying information is appropriate.

1.5 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, submission of required safeguard reports to the IRS, properly reporting any data breach incidents, disclosure awareness training and for any necessary liaison with the IRS.

1.6 Safeguard Reviews

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

- **On-site reviews**: Disclosure Enforcement Specialists (DES), Cybersecurity Reviewers (CSR), and Management Officials will conduct an on-site evaluation of the security and privacy controls implemented by the agency and all supporting parties. Assessment techniques include, but are not limited to visual inspections, observations, interviews, document exchange, and automated scanning.

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

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

1.6.1 Before the Review

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

This engagement letter outlines what the review will encompass. 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, policies, awareness program documentation and organizational charts relating to the processing of FTI). Prior to the review, the agency POC will receive information regarding the manner in which the review will be conducted (e.g., on-site and/or remote), the

scope and purpose of the review, a list of the specific areas to be reviewed and agency personnel to be interviewed.

A Preliminary Security Evaluation (PSE) call will be held to determine the scope of the review (see NIST Control PM-5 CE-1, Inventory of PII). The electronic flow of FTI will be discussed to provide the review team with a thorough understanding of the location and use of FTI throughout the agency's infrastructure. During the call primary POCs will be introduced, the scope of the review will be defined, assessment logistics will be discussed, and any questions will be answered. Participants should include agency IT staff knowledgeable about the location and flow of FTI throughout the agency as well as staff or contractors from other locations such as consolidated data centers. Additionally, mini-PSE calls for contractors, sub-contractors, off-site locations, etc. may be needed to obtain additional information in determining the review scope. Requests for additional information and clarification to include automated scanning procedures will be discussed after the PSE call(s) and a proposed scope will be provided.

1.6.2 During the Review

The review process validates the accuracy of the SSR and conformance with the current version of Publication 1075 requirements and National Institute of Standards and Technology (NIST) Special Publication 800-53. At the opening conference, review procedures will be communicated, followed by a data flow discussion, and confirming the flow of FTI (see NIST Control PM-5 CE-1, Inventory of PII). Observing actual operations is a required step in the review process. Sites to be reviewed will be based on the flow of the FTI, which may include, but are not limited to, field offices, consolidated data centers, off-site storage facilities, disaster recovery sites, contractor and sub-contractor sites.

Review methods may include but are not limited to:

- Spot check agency records for FTI
- Employee interviews
- Facility tours
- Document review
- Automated/manual testing (See Safeguards website for tools used for automated testing)
- Remote assessment tools

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

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

The closing conference is held upon completion of the agency's review, where the PFR is issued to provide the agency an overview of the findings identified during the review.

1.6.3 After the Review

An SRR and CAP will be issued within 45 days of the closing conference to document the review findings. Requests for corrections to the SRR must be emailed to the SafeguardReports@irs.gov mailbox. The Office of Safeguards will respond with an acknowledgement and a determination.

Each finding will be identified with a criticality level that identifies potential risk to loss, breach or disclosure of FTI.

Safeguards Finding Criticality Definitions

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

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.

If the Agency has any critical findings, the agency must submit a mitigation plan to Safeguards within 7 days from the closing conference date. Safeguards will report the critical findings along with your agency plan to the Treasury Inspector General for Tax Administration (TIGTA).

The CAP must be updated and submitted semi-annually using the last CAP issued by the Office of Safeguards (see Section 2.E.5, Corrective Action Plan) until all review findings are accepted as closed.

If an agency has a CAP due within 60 days of the review, that CAP is not required because the remaining open findings will be handled as part of the upcoming on-site or remote Safeguard Review

Each CAP submission must include an explanation and/or evidence of actions already taken or planned to resolve all outstanding findings. The agency must submit an actual or planned implementation date for each outstanding finding.

1.7 Termination of FTI

1.7.1 Agency Request

1.7.1.1 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 2.F Disposal of FTI – IRC § 6103(p)(4)(F))

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

1.7.1.2 Archiving FTI Procedure

This section is for agencies terminating receipt of FTI but required by statute to retain FTI for designated periods. If residual FTI is required to be retained by statute for a designated period (e.g., 5 or 10 years), then agencies must:

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

1.7.2 FTI Suspension, Termination and Administrative Review

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

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

Prior to terminating FTI, the IRS will notify the authorized recipient in writing and may suspend further disclosures if it is deemed that federal tax administration would be seriously impaired.

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

1.8 Reporting Improper Inspections or Disclosures

1.8.1 Terms

1.8.1.1 Data Incident

A data incident is an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures or acceptable use policies. Incidental and inadvertent accesses are considered data incidents.

An incident involving the loss or theft of an IRS asset containing FTI, or the loss or theft of a physical document that includes FTI, or the inadvertent disclosure of FTI, is known as a data breach. See the Data Breach definition below. Often, an occurrence may be first identified as an incident, but later identified as

a data breach once it is determined that the incident involves FTI. This is often the case with a lost or stolen laptop or electronic storage device.

1.8.1.2 Data Breach

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

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

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

Some common examples of a data breach include:

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

1.8.2 General

A written policy must be established and distributed that covers incident management. The policy must clearly state the actions that will be taken for the improper inspection or disclosure of FTI. Upon discovering a possible improper inspection or disclosure of FTI, including breaches and incidents, by a federal employee, a state employee or any other person, the individual making the observation or receiving information must contact the local Treasury Inspector General for Tax Administration (TIGTA) Field Division office, to the Special Agent-in-Charge, immediately, but no later than 24 hours after identification of a possible issue involving FTI. See NIST IR-6, Incident Reporting and IR-8, Incident Response Plan.

Local TIGTA Field Division Office contact information can be found on the TIGTA website at https://www.treasury.gov/tigta/oi_office.shtml.

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

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

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

TIGTA Homepage: https://www.treasury.gov/tigta

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

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

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

1.8.3 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 or breach known at that time into a data incident report, including but not limited to:

- Name of agency and agency POC for resolving data incident with contact information
- Date and time the incident/breach occurred
- Date and time the incident/breach was discovered
- How the incident/breach was discovered
- Description of the incident/breach and the data involved, including specific data elements, if known
- Potential number of FTI records involved; if unknown, provide a range if possible
- Address where the incident/breach occurred
- IT involved (e.g., laptop, server, mainframe)
- Does the incident involve an unauthorized access or disclosure by an agency employee? (Y/N)

- If a criminal indictment is not pursued, will a disciplinary or adverse action be proposed against the agency employee involved in this unauthorized access or disclosure? (Y/N)

Reports must be sent electronically and encrypted via IRS-approved encryption techniques as outlined in Section 2.E.3, Encryption Requirements. 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.

1.8.4 Incident Response Procedures

In the event of an unauthorized disclosure or data breach, the agency must contact TIGTA and the IRS immediately. Both TIGTA and the IRS must be contacted within 24 hours of the discovery of the disclosure or breach. The agency must not wait to conduct an internal investigation to determine if FTI was involved. Any internal investigation conducted by the agency should not delay the timely reporting of the disclosure or breach.

Incident response policies and procedures required in NIST Control IR-1, Incident Response Policy and Procedure, 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 must be resolved as soon as reasonably possible. Additional training on any changes to the incident response policies and procedures must be provided to all employees, including contractors, sub-contractors and consolidated data center employees, immediately. See NIST Control IR-4, Incident Handling for additional information.

The agency must test the incident response capability annually using tabletop exercises to determine the incident response effectiveness and document the results. See NIST Control IR-3, Incident Response Testing.

The agency must track and document system security and privacy incidents. See NIST Control IR-5, Incident Monitoring.

1.8.5 Incident Response Notification to Impacted Individuals

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

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

1.9 Disclosure to Other Persons

1.9.1 General

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

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

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

1.9.2 Authorized Disclosure Precautions

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

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

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

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

1.9.3 External Personnel Security

An external provider refers to organizations other than the agency operating or acquiring the system. External providers include, for example, contractors or sub-contractors and other organizations providing system development, information technology services, outsourced applications, testing/assessment services and network and security management. Agencies must include personnel security requirements in contracts. External providers may have personnel working at agency facilities with credentials, badges or system privileges. Notifications of external personnel changes ensure appropriate termination of privileges and credentials. See NIST Control PS-7, External Personnel Security.

1.9.4 Disclosing FTI to Contractors or Sub-Contractors

The agency must notify the Office of Safeguards prior to re-disclosing FTI to contractors or sub-contractors. The agency must notify and obtain written approval from the Office of Safeguards prior to re-disclosing FTI to sub-contractors (when the agency's contractor uses or desires to re-disclose FTI to another contractor). See Section 2.E, Reporting Requirements - 6103(p)(4)(E) and Section 2.E.6, Notification Reporting Requirements, for additional information.

In addition to the notification, the agency must:

- Establish privacy roles and responsibilities for contractors or sub-contractors and service providers to safeguard the confidentiality and integrity of FTI.
- Include privacy requirements in contracts and other acquisition-related documents.
- Share FTI externally only for the purposes statutorily authorized.
- 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.
- 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.
- Require agency notification of contractor or sub-contractor personnel changes to ensure appropriate termination of privileges and credentials. See NIST Control PS-7, External Personnel Security.
- Evaluate any proposed new instances of sharing FTI with third parties to assess whether they are authorized.
- Require contractor or sub-contractor employ a formal sanction process for contractor employees and, when permitted by statute, sub-contractor employees failing to comply with established information security policies and procedures for FTI. Notification of designated agency personnel is required within 72 hours.

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

The Taxpayer First Act § 2004, which added IRC § 6103(p)(9), formalizes in statute the following agency requirements effective December 31, 2022:

- Agencies must require that contractors, sub-contractors, or other agents have requirements in effect to provide safeguards required under IRC § 6103(p)(4) to protect FTI.
- The Taxpayer First Act also codifies agency responsibilities to conduct **on-site** reviews of contractors, sub-contractors, and other agents and provide the findings of these reviews to Safeguards as part of the report required under IRC § 6103(p)(4)(E).
- Agencies will provide the Office of Safeguards with an annual certification that each contractor, sub-contractor, or other agent is in compliance with the above requirements. This certification will be included as part of the report required under IRC § 6103(p)(4)(E).

- Agency requirements for this new legislation will be issued prior to implementation in the form of an Interim Guidance memorandum.

1.9.5 Re-Disclosure Agreements

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

Agreements must include language to enforce the requirements for:

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

Federal agencies authorized by statute to enter into re-disclosure agreements are required to provide a list of all executed agreements annually in the SSR. When requested by the Office of Safeguards, agencies must provide a copy of all re-disclosure agreements within 30 days. An electronic copy must be sent to the Office of Safeguards via SDT. If SDT is not available, the agreements may be emailed to the SafeguardReports@irs.gov mailbox.

1.10 Return Information in Statistical Reports

1.10.1 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 fewer than five returns may be released.
- Statistical tabulations prepared at the state level may not be released for cells containing data for fewer than 10 returns. Data for geographic areas below the state level such as county may not be released with cells containing data from fewer than 20 returns. In addition, for tabular data at the ZIP Code level, additional procedures must be employed. Individual ZIP Code areas with fewer than 100 returns cannot be shown. Additionally, any cell in the ZIP Code table based on fewer than 20 returns cannot be shown. Finally, individual returns that represent a large percentage of the total of a particular cell must be excluded from the data.
- Tabulations that would pertain to specifically identified taxpayers or that would tend to identify a particular taxpayer, either directly or indirectly, may not be released.

1.10.2 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

1.10.3 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[2] and complete a Need and Use Justification for Federal Tax Information Form.

2. The completed and signed form must be returned to the IRS disclosure manager for review and approval. The Office of Safeguards will be notified by the IRS disclosure manager of the request and approval.

3. Changes to the terms of the statistical analysis activities documented in the form must be submitted to the IRS Office of Safeguards as part of the annual SSR (see Section 1.4, State Tax Agency Limitations and Section 2.E.4, Safeguard Security Report).

4. Updates to the form must be made as requested by the IRS disclosure manager.

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

[2] Refer to https://www.irs.gov/privacy-disclosure/irs-freedom-of-information for contact information.

2.0 PHYSICAL SECURITY REQUIREMENTS

2.A Recordkeeping Requirement – IRC § 6103(p)(4)(A)

2.A.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 a minimum of five (5) years. 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.

2.A.2 Logs of FTI (Electronic and Non-Electronic Receipts)

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 the following tracking elements:

- Taxpayer 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 safeguarding requirements.

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

- Reflect to whom the disclosure was made
- What was disclosed
- Why it was disclosed
- 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 Logs

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

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

2.A.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 2.A.2, Logs of FTI, (Electronic and Non-Electronic Receipts) depending upon the current form of the FTI, electronic or non-electronic.

2.A.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 2.A.2, Logs of FTI, (Electronic and Non-Electronic Receipts).

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

2.B Secure Storage – IRC § 6103(p)(4)(B)

2.B.1 General

Security may be provided for a document, an item, or an area in several 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 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.

2.B.2 Minimum Protection Standards

MPS establishes 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 must be used as a starting point to identify two barriers of MPS to protect FTI.

Table 1 – 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, locked IT cabinet) with a resistance to forced penetration, and a security lock with controlled access to keys or combinations.

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

As an example, an agency often desires or requires that security personnel, custodial service workers, or landlords for non-government-owned facilities have access to locked buildings and rooms. This may be permitted if 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 NIST Special Publication (SP) 800-53 Revision 5. These are identified in Section 4.0, NIST 800-53 Security and Privacy Controls. Per NIST guidelines, policies and procedures must be developed, documented and disseminated, as necessary, to facilitate implementing physical and environmental protection controls.

Multifunction Devices (MFDs) or High-Volume Printers must be locked with a mechanism to prevent physical access to the hard disk or meet MPS.

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

2.B.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 must either 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, disclosure, or theft of FTI. All 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.

2.B.3.1 Visitor Access Logs

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

Prior to accessing areas that contain FTI, a visitor must sign a visitor access log. The security personnel must validate the person's identity by examining government-issued identification (e.g., state driver's license or passport). 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.

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

Each restricted area access log must be closed out at the end of each month and reviewed by management. Visitor access logs must be retained for five (5) years, see Exhibit 9, Table 9.

Figure 2 – Visitor Access Log

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

2.B.3.2 Authorized Access List

To facilitate the entry of employees/vendor/contractor/non-agency personnel who have a frequent and continuing need to enter a restricted area, but who are not assigned to the area, an Authorized Access List (AAL) can be maintained so long as MPS are enforced. See Section 2.B.2, Minimum Protection Standards.

The AAL must contain the following:

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

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

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

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

2.B.3.3 Controlling Access to Areas Containing FTI

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

The agency must maintain a policy addressing issuance of appropriate authorization credentials, including badges, identification cards or smart cards. This policy must include proper use and accountability requirements.

In addition, a list must 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 must control physical access to the information system devices that display FTI information or where FTI is processed to prevent unauthorized individuals from observing the display output. For additional information, see NIST Control PE-5, Access Control for Output Devices.

The agency or designee must monitor physical access to the information system where FTI is stored to detect and respond to physical security incidents. For additional information, see NIST Control PE-6, Monitoring Physical Access.

For all areas that process FTI, the agency must position information system components within the facility to minimize the opportunity for unauthorized access.

When cleaning and facility maintenance personnel work in restricted areas containing unsecured FTI, those activities must be performed in the presence of an authorized employee.

The agency must establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel. The agency must verify that non-escorted personnel performing maintenance on the system possess the required access authorizations and if not, then the agency must designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities. See NIST MA-5, Maintenance Personnel.

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.

2.B.3.4 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 when the key or combination is controlled. Compromising a combination or losing a key negates the security provided by that lock. Combinations to locks must be changed annually or when an employee who knows the combination retires, terminates employment or transfers to another position.

Combinations 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 using the same security measures for the envelope as the locked material.

Access control measures (keys, proximity cards, combinations) must be issued only to individuals having a need to access an area, room, or container. Inventory records must be maintained and must account for the total number of keys, proximity cards, combinations, etc. that are available and issued. The inventory must account for master keys and key duplicates. An annual reconciliation must be done on all key records.

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

2.B.3.5 Locking Systems for Secured Areas

Access control systems (e.g., badge readers, smart cards, and biometrics) that provide the capability to audit access control attempts must maintain access control logs 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

2.B.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 microform) 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 must not be labeled as FTI or provide any indication that the contents contain FTI, since that may actually increase risk to the contents.

2.B.4.1 Security During Office Moves

When it is necessary for an office to move to another location, plans must be made to protect and account for all FTI properly. FTI must be in locked cabinets or sealed packing cartons while in transit. Using sealed boxes serves the same purpose as double-sealing and prevents anyone from viewing the contents. FTI must remain in the custody of an agency employee and accountability must be maintained to ensure that cabinets or cartons do not become misplaced or lost during the move.

2.B.5 Physical Security of Computers, Electronic and Removable Media

Computers and electronic media (including telephones using Voice Over Internet Protocol [VOIP]) that receive, process, store, access, protect and/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.

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 computers, electronic and removable media must be maintained and reviewed semi-annually for control and accountability. Section 2.A, 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 NIST Control PE-4, Access Control for Transmission.

2.B.6 Media Off-Site Storage Requirements

Media containing FTI that is sent to an off-site storage facility must be properly secured, labeled, and always protected from access by unauthorized individuals. The media may not be stored on open shelving, unless the shelving is in a restricted area (see Section 2.B.3, Restricted Area Access) 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, and employee training) and the contract must include Exhibit 7 safeguarding language. These facilities are subject to IRS safeguard reviews.

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

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

2.B.7 Alternate Work Site

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 the requirements of Section 2.B.5, Physical Security of Computers, Electronic and Removable Media, apply to alternate work sites.

2.B.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 present at 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 3.3.7 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 ensure employees have access to 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 alternate 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.

2.B.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.

2.B.7.3 Other Safeguards

Only agency-approved security access control devices and agency-approved software will be used. Use of illegal and/or non-approved software is prohibited. Electronic media that is to be reused must follow media sanitization requirements.

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 must certify that the security controls are adequate for security needs. Additionally, the agency must develop and disseminate 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.

2.C Restricting Access – IRC § 6103(p)(4)(C)

2.C.1 General

Agencies are required by IRC § 6103(p)(4)(C) to restrict access to FTI to only 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 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 Section 4.14 Program Management (PM) and Exhibit 8, Warning Banner Examples).

Auditing controls, with the capability to generate records, to detect browsing within all systems that receive, process, store, access, protect and/or transmit FTI (i.e., TDS, case management systems, etc.) must be implemented. See NIST Sections AU-6 Audit Review, Analysis and Reporting, AU-7, Audit Reduction and Report Generation and AU-12, Audit Generation, for additional requirements.

To understand the key terms of access, unauthorized disclosure, unauthorized access and need-to-know, see section on Key Definitions.

2.C.2 Policies and Procedures

Agencies must maintain the following policies and procedures relating to the safeguarding of FTI. For policies and procedures to be current, they need to have been updated or revalidated within the last three (3) years.

- **Alternate Work Site** – See Section 2.B.7 Alternate Work Sites
  If permitted, a policy/procedure must address the security of FTI at alternate work sites. A policy is required even if alternate work sites are prohibited.

- **Email** – See Section 3.3.2 Email Communications
  A policy/procedure must address the proper protection of FTI when transmitted by email, or if emailing of FTI is not allowed, a policy must state that it is prohibited.

- **Facsimile -** See Section 3.3.3 Facsimile and Facsimile Devices
  A policy/procedure must address the proper protection of FTI when transmitted by facsimile, or if facsimile transmission of FTI is not allowed, a policy must state that it is prohibited.

- **Employee Badge** – See Section 2.B.2 and Table 1 Minimum Protection Standards
  The policy/procedures must address when employees serve as secondary barriers for safeguarding FTI, picture identification badges or credentials must be visible and worn above the waist.

- **FTI Disposal/Destruction** – See Sections 2.A.2 FTI Logs, (Electronic and Non-Electronic Receipts), 2.F.3 Destruction and Disposal, 2.F.4 Other Precautions and 2.F.3.1 Media Sanitization
  The policy/procedures must address the proper safeguarding of FTI including the tracking and the schedule/method of disposal or destruction.

- **Incident Response** – See NIST Control IR-1 and Sections 1.8.4 Incident Response Procedures
  The policy/procedures must include the proper response to identified unauthorized disclosure or data breach incidents.

- **Internal Inspections** – See Sections 2.D.3 Internal Inspections and 2.D.9 Plan of Action and Milestones
  The policy/procedures must include a documented schedule to ensure that all internal inspections are conducted timely. Additionally, a POA&M must be developed and monitored, including tracking the corrective actions identified during the internal inspections and identified actions planned to resolve the findings.

- **Restricting Use of Personally Owned Computers** – See Section 2.B.7.1 Equipment
  The policy/procedures must include only agency-owned computers, media and software used to process, access and store FTI.

- **Disclosure Awareness, Security and Privacy, Role-Based and Contingency Training** – See Sections 2.D.2 Training Requirements, 2.D.2.1 Disclosure Awareness Training, NIST Controls AT-2 Awareness Training, AT-3 Role-Based Training and CP-3 Contingency Training
  These policies/procedures must contain a signed certification by the employee or contractor stating they understand the security policy and procedures for safeguarding FTI, prior to access to FTI.

- **Transcript Delivery System (TDS) Audit Log Review (if applicable)** – See Section 4.1, Access Control

The policy/procedures must address the development, documentation, and dissemination of audit/accountability security controls.

- **Background Investigation** – See Section 2.C.3 Background Investigation Minimum Requirements
  The policy/procedure requires that employees, contractors, and sub-contractors (if authorized) with access to FTI must have a background investigation completed and favorably adjudicated.

- **Access Control** – See Section 2.B.3.3 Controlling Access to Areas Containing FTI and NIST Control AC-1, Access Control Policy and Procedures.
  The policy/procedures must address the issuance of appropriate authorization credentials, including badges, identification cards or smart cards and include proper use and accountability requirements. The policy/procedures must also include the prohibition of allowing individuals to "piggyback" or "tailgate" into any location containing FTI.

- **Audit and Accountability -** see NIST Control AU-1, Audit and Accountability Policies and Procedures
  The policy/procedures must address purpose, scope, roles, responsibilities, compliance, management commitment and coordination among organizational entities. Agencies must develop, document, and implement remediation actions for violations of the audit and accountability policy.

- **Media Protection** – see NIST Control MP-1, Media Protection Policies and Procedures
  The policy/procedures must cover the protection of media to include access, marking, storage, transport, use and sanitization. See NIST Controls MP-1 through MP 7.

- **Physical and Environmental** – See NIST Control PE-1
  The policy/procedures must include a clean desk policy for the protection of FTI; designate restricted IT areas that house IT assets such as, but not limited to, mainframes, servers, controlled interface equipment, associated peripherals, and communications equipment; and address specific building access systems, as needed.

- **Personnel Security** – See NIST PS-1, Personnel Security Policy and Procedures
  The policy/procedures must address position risk designation, personnel screening, personnel termination, personnel transfer, access agreements and personnel sanctions.

- **Insider Threat Program**– See NIST Control PM-12, Insider Threat Program
  The policy/procedures must address an insider threat program that includes a cross-discipline insider threat incident handling team and designate a senior official as the responsible individual to implement and provide oversight for the program.

- **Privacy Program Plan**[3] – See NIST Control PM-18, Privacy Program Plan
  A privacy program plan is a formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program and the program management and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

[3] NIST Privacy Control

2.C.3 Background Investigation Minimum Requirements

Determining the suitability of individuals who require access to U.S. government 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 that is favorably adjudicated by the Agency and to include, at a minimum, the following requirements:

- 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 Federal Investigative Standards (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 that defines what would result in preventing or removing an employee's, contractor's and sub-contractor's access to FTI.

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

- State agencies must ensure a reinvestigation is conducted within five (5) years from the date of the previous background investigation for each employee, contractor, and sub-contractor requiring access to FTI.

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

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

    1. 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.

    2. Check of local law enforcement agencies where the subject has lived, worked, and/or attended school within the last five (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.

    3. 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 three (3) days of completion, any new employee must also be processed through E-Verify to assist with verification of their 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.

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 FIS. Granting access to FTI requires, at a minimum, a Tier 2 level investigation.

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, contractor, and sub-contractor with access to FTI. Federal agencies may be asked to provide evidence that the required background investigation was conducted for each individual granted access to FTI. FIS standards require reinvestigation, at a minimum, every five (5) years.

State and local agencies that 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 above as the minimum standard, with a reinvestigation conducted within five (5) years from the previous investigation.

2.C.3.1 Background Investigation Requirement Implementation

Agencies must establish a written background investigation policy that conforms to the standards of Section 2.C.3. Agencies must also identify all employees, contractors, and sub-contractors who currently have access to FTI and have not completed the required personnel security screening and initiate a background investigation that meets these standards. Agencies must initiate a background investigation for all newly hired employees, contractors, and sub-contractors who will require access to FTI to perform assigned duties. All adjudications must be done by the agency or another state agency delegated to perform, such as an Office of Administration or HR agency.

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 must be initiated for continued access to FTI.

2.C.4 Personnel Actions

2.C.4.1 Personnel Transfer

When reassignments or transfers of individuals are permanent or of such extended durations certain actions are warranted. Agencies must define actions appropriate for these types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example, returning old and issuing new keys, identification cards and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and access to official records to which individuals

had access at previous work locations and in previous system accounts. See NIST Control PS-5, Personnel Transfer.

2.C.4.2 Personnel Sanctions

Agencies must document in policy and procedure a formal sanctions process for individuals failing to comply with established information security policies and procedures. Agencies must notify designated agency personnel within 72 hours when a formal employee sanction process is initiated, identifying the individual sanctioned and any required administrative actions. See NIST Control PS-8, Personnel Sanctions.

When the formal sanction is a proposed disciplinary or adverse action involving an unauthorized access or disclosure of FTI, the agency must provide written notification to the taxpayer whose FTI was subject to unauthorized access or disclosure. The required written notification must include the date the unauthorized access or disclosure of FTI occurred and the rights of the taxpayer under IRC § 7431 (see Section 1.8.5, Incident Response Notification to Impacted Individuals).

2.C.4.3 Personnel Termination

In personnel termination situations, certain actions are required. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, agencies must consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified.

Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. System-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards and building passes. See NIST Control PS-4, Personnel Termination.

2.C.5 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 a sentence of text in a paper notice or letter; a row or column containing FTI in a database table; files stored on electronic media where some contain FTI and some do not; or at a shared data center where some systems contain FTI that require access restrictions, and some do not. Any kind of commingling creates the need for additional controls, since the introduction of FTI requires the entire letter, data table, removable media, etc. 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.

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 taxpayer or third party subsequently provides the address independently, the address will not be considered FTI as long as the address is overwritten using individual or third-party knowledge or records as the source of information to replace the IRS source address.

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

2.C.5.1 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.

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 NIST Control MP-3, Media Marking
- When technically possible, data files, data sets and shares must be overwritten after each use

Commingled data at multi-purpose facilities results in security and privacy 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 physical and systemic controls must be maintained to prevent unauthorized disclosure of this information.

2.C.6 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[4].

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 (IRC § 6103(d)) and a component

[4] Refer to https://www.irs.gov/privacy-disclosure/irs-freedom-of-information for contact information.

human services agency administering benefit eligibility verification programs (IRC § 6103(l)(7)) or child support enforcement programs (IRC § 6103(l)(6)).

2.C.7 Offshore Operations

FTI cannot be accessed by agency employees, agents, representatives, contractors, or sub-contractors located outside of the legal jurisdictional boundary of the United States (outside of the United States, its territories, embassies, or military installations). FTI must not be received, processed, stored, accessed, or transmitted to (IT) systems located offshore nor may FTI be sent offshore for disposal. Systems containing FTI must be located, operated and maintained by personnel physically located within the United States (this prohibits foreign remote maintenance, foreign call centers, help desks and the like) and should follow Publication 1075 requirements including the Background Investigation Requirements in Section 2.C.3.

Some agencies may have a need for their employees to travel internationally for business purposes. As such, agencies must develop procedures to follow during foreign travel. When agency employees travel abroad, they must not:

- Bring IT equipment containing stored FTI (e.g., laptop computers, tablets, phones, removable media); or
- Access agency systems that receive, process, store, protect and/or transmit FTI.

During international travel, batteries of agency-managed or Bring Your Own Device (BYOD) mobile devices and laptops must be removed from battery-powered mobile devices and stored separate from the device when left unattended. SIM cards must be removed and stored separate from devices that employ them when entering non-U.S. customs. Once agency employees return from abroad, it is important for agencies to ensure the continued security of networks where FTI resides. Agencies must sanitize all devices taken abroad prior to allowing them to connect to their trusted network. Additionally, agencies must disable wireless connectivity options until devices have been sanitized and may wish to provide additional security training for employees travelling abroad.

2.C.8 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 environments listed in 2.C.8.1 and 2.C.8.2.

2.C.8.1 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.

2.C.8.2 Agency, Contractor or Sub-Contractor Shared Facilities

Recipients of FTI are permitted 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 and sub-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 or sub-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.

The agency, as well as its contractor, sub-contractor and shared sites that receive, process, store, access, protect and/or transmit FTI, are subject to Safeguard reviews.

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

2.C.9 Service Level Agreements (SLA)

Agencies using support functions, including, but not limited to, consolidated data centers, shared print facilities, and disaster recovery sites, must implement appropriate controls to ensure the protection of FTI. This includes a service level agreement (SLA) between the agency authorized to receive FTI and support functions. The SLA must cover the following:

- The agency with authority to receive FTI is responsible for ensuring the protection of all FTI received. The state support function shares responsibility for safeguarding FTI.
- The Exhibit 7 language must be included in the SLA between the recipient agency and support functions and in all contracts involving contractors or sub-contractors hired by the state support function.
- The SLA provides written notification to the state support function’s 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’s right to inspect state support function facilities and operations receiving, processing, storing, accessing, protecting and/or transmitting FTI under this agreement to assess compliance with requirements defined in IRS Publication 1075. The SLA shall specify that IRS’s 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 state support function’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 state support function every 18 months, as described in Section 2.D.3, Internal Inspections. Multiple agencies sharing a state support function such as 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 state support function with access to or use of FTI, including system administrators and programmers, must:

1. Meet the background check requirements defined in Background Investigation Minimum Requirements and

2. Receive disclosure awareness training and sign a confidentiality statement, prior to initial access to or use of FTI, as well as annually thereafter. These provisions also extend to any contractors or sub-contractors hired by the state support function that have authorized access to or use of FTI.

- The specific data breach incident reporting procedures for all state support function employees, contractors and sub-contractors must be covered. The required disclosure awareness training must include a review of these procedures.

- Responsibilities must be identified for coordination of the 45-day notification of the use of contractors or sub-contractors with access to FTI.

- Require a formal sanction process for individuals covered by the SLA for failing to comply with established FTI security policies and procedures. Notification of designated agency personnel is required within 72 hours when the formal sanction is a proposed disciplinary or adverse action involving an unauthorized access or disclosure of FTI and must include the date the unauthorized access or disclosure of FTI occurred.

Generally, consolidated data centers are operated either by a separate state agency (e.g., Department of Information Services) or by a private contractor or sub-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.

2.C.10 Review Availability of Contractor and Sub-Contractor Facilities

As part of the agency review process, all affiliated contractors and sub-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 for all contracts.

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

2.C.11 Restricting Access – Other Disclosures

2.C.11.1 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, contractors or sub-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, contractor, or a sub-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

- 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, contractor, or sub-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.

Additional information regarding the use of FTI for child support enforcement purposes can be found at: https://www.irs.gov/privacy-disclosure/use-of-federal-tax-information-fti-for-child-support-enforcement-purposes-matrix

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

2.C.11.2 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 or sub-contractors.

2.C.11.3 Deficit Reduction Agencies—IRC § 6103(l)(10)

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

2.C.11.4 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.

2.C.11.5 Disclosures under IRC § 6103(l)(20)

Disclosures to officers, employees, contractors, and sub-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 and any redisclosures authorized by this provision are subject to safeguards requirements.

2.C.11.6 Disclosures under IRC § 6103(l)(21)

Disclosures to officers, employees, contractors, and sub-contractors of the U.S. Department of Health and Human Services (HHS) are 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 safeguards requirements. Any agent contractor, or sub-contractor is also subject to IRS safeguard requirements and review.

IRC § 6103(l)(21)(C) may allow HHS Office of Inspector General 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 that may not have access to FTI in eligibility records unless a contractual relationship is established that conforms to the disclosure requirements of IRC § 6103.

2.C.11.7 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 safeguards requirements and review.

The Department of Justice (DOJ) 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.

2.C.11.8 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, contractors, or sub-contractors, the agency and agents, contractors, or sub-contractors are all subject to IRS safeguarding requirements and reviews.

2.D Other Safeguards - IRC § 6103(p)(4)(D)

2.D.1 General

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

2.D.2 Training Requirements

Education and awareness are necessary to provide employees, contractors, sub-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 the requirements to comply with this publication.

Disclosure awareness training is described in detail within Section 2.D.2.1, Disclosure Awareness Training. Additional training requirements are located in various sections of the document and identified in the following table.

Table 2 – Training Requirements

Training Component	Applicability	Section
Disclosure Awareness Training	• Specific to protection of FTI and prevention of unauthorized disclosure	2.D.2.1
Security and Privacy Awareness Training	• Provides basic security and privacy awareness training to information system users	AT-2
Role-Based Training	• Provides individualized training to personnel based on assigned security roles and responsibilities	AT-3
Contingency Training	• Provides individualized training to personnel based on assigned roles and responsibilities as they relate to recovery of backup copies of FTI	CP-3
Incident Response Training	• Provides individuals with agency-specific procedures to handle incidents • Provides individuals with IRS-specific requirements pertaining to incidents involving FTI	IR-2 and 1.8
Insider Threat Awareness Training	• Provides individuals with agency-specific procedures to increase insider threat awareness	PM-12

2.D.2.1 Disclosure Awareness Training

Prior to granting an authorized agency employee, state support employee, contractor, or sub-contractor access to FTI, or to systems containing FTI, each employee, contractor, or sub-contractor must certify their understanding of the agency's security and privacy policy and procedures for safeguarding FTI through the agency's disclosure awareness training. The use of FTI in any training environment, including Disclosure Awareness training or material, is prohibited.

Disclosure awareness training (including role-based training) must provide personnel who have access to FTI with initial and annual training on:

- Organizational authority for receiving FTI
- Authorized uses of FTI
- Disclosure of FTI with external parties only when authorized

- Consequences of unauthorized access, use or disclosure of FTI

Employees, contractors, and sub-contractors must be advised of the penalty provisions of IRC §§ 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 1.8, Reporting Improper Inspections or Disclosures).

During this training, agencies must make employees, contractors, or sub-contractors aware that disclosure restrictions and penalties apply even after employment or contract with the agency has ended.

For the initial certification, and each annual recertification thereafter, the employee, contractor or sub-contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their 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 within 24 hours.

> 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 (5) years.

The agency must include practical exercises in awareness training that simulate security and privacy incidents. Practical exercises may include, for example, social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Privacy-related practical exercises may include, for example, practice modules with quizzes on handling FTI and affected individuals in various scenarios. See NIST Control AT- 2 (CE1).

The agency must include role-based security and privacy training, including insider threat awareness, to personnel with access to FTI. Role-based training for security and privacy may include, for example, security and privacy training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities, or spear/whale phishing attacks targeted at senior leaders/executives. Role-based training on handling FTI helps prevent unauthorized collections or uses of FTI. See NIST Control AT-3 (CE3 and CE5)

At least once per quarter, agencies must distribute security and privacy awareness reminders/updates to all users. This is in addition to annual awareness training. Security and privacy awareness updates can be disseminated to appropriate personnel by using a variety of methods, such as, but not limited to:

- Email and other electronic messages to inform users
- 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)
- Additional formal and informal training

2.D.2.2 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 and please provide the publication number and quantity. Please note that all Notice 129 quantities are ordered by pad or roll count (100 pieces per, so 10 rolls = 1,000 labels). 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) but, if you experience an ordering problem, obtain the employee’s name and ID number and send an email to SafeguardReports@irs.gov mailbox so the Office of Safeguards can assist you.

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

UNAX is Serious 11" x 17” Poster
Available through Distribution Center: Document 12800

Stop UNAX In Its Tracks Tri-fold handout
Available through Distribution Center: Document 12612

Publication 1075, Tax Information Security and Privacy Guidelines for Federal, State and Local Agencies (Key publication explains the federal safeguard requirements)
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)[5]
Available online through Safeguards website: https://www.irs.gov/uac/irs-disclosure-awareness-videos

2.D.3 Internal Inspections and On-Site Reviews

Another measure IRS requires for the safeguarding of FTI is internal inspections by the recipient agency. The purpose is to ensure that the security and privacy policies and procedures established by the agency to protect FTI are functioning, maintained, and enforced. The agency must submit copies of these inspection reports (see Internal Inspection Template on the Office of Safeguards website) to the IRS with the SSR (see Section 2.E.4, Safeguard Security Report). To provide an objective assessment, the inspection should be conducted by agency personnel outside the FTI using function being inspected.

[5] The use of the Safeguards Disclosure Awareness Video does not completely satisfy the training requirements of NIST 800-53 Revision 5.

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

In a situation where it is unwieldy or otherwise not feasible for agency leadership to personally conduct the inspection, it is permissible for off-site locations with access to FTI to self-certify the internal inspection. If possible, the agency should make an initial visit to the off-site location prior to disclosing FTI and conduct an initial inspection. The agency must ensure the self-certified inspection is signed by an agency employee, received timely, reviewed thoroughly, have in-depth discussions with the person conducting the self-certification and submit the self-certified inspections with the agency SSR.

Contractors and sub-contractors may not conduct self-certification internal inspections.

Agencies must establish a review cycle as follows:

- Field offices receiving FTI at least every three (3) years
- Headquarters office facilities housing FTI and the agency computer facility at least every 18 months
- All contractors and sub-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 2.E.4.

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 a 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.

Required items to review during internal inspections include recordkeeping, secure storage, limited access, disposal, and cybersecurity.

2.D.4 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.

2.D.5 Secure Storage

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

2.D.6 Limited Access

Access to returns and return information (including tapes, cartridges, or other removable media) must be limited to only those employees, officers, contractors, and sub-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.

2.D.7 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 2.F, Disposing of FTI - IRC § 6103(p)(4)(F).

2.D.8 Computer Systems Security

The agency's review of the adequacy of its cybersecurity 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 4.1, Access Control, and other portions of Section 3.0, Cyber security Requirements, as applicable).

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

2.D.9 Plan of Action and Milestones (POA&M)

The agency must implement a process for ensuring that corrective actions are developed and monitored. The process must include the findings identified during the internal inspections and the remediation plans and dates to resolve these findings.

Although similar, the IRS CAP covers findings identified by the Office of Safeguards during the safeguard review and would not include or track agency findings from the internal inspection process.

2.E Reporting Requirements – IRC § 6103(p)(4)(E)

2.E.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, accessed, protected, and/or transmitted to or from the agency. The major reporting requirements include the SSR, CAP and 45-day notification.

2.E.2 Report Submission Instructions

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

- 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 2.E.3, Encryption Requirements.

Agencies must follow the requirements below when submitting correspondence, reports, and attachments to the Office of Safeguards:

- Submissions must include a signed certification letter from the Head of Agency or a designee. In the event the agency submits a report signed by a designee, there must be a delegation of authority signed by the Head of Agency (HOA).
- All correspondence requiring HOA signature must be in the form of a handwritten (aka. Wet) signature or a digital certificate signature. The HOA can delegate individuals to sign these

documents on their behalf. To do so, the HOA must provide a delegation of authority for individual they will assign as their designee. The delegation of authority must be kept current by the agency and retained for at least three years and will be reviewed by IRS personnel during Safeguard reviews.

- Submissions must be made using official templates provided by the Office of Safeguards.
- Reports referencing file attachments must 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, either by a logical order (e.g., CAPATT1, CAPATT2) or by finding number (e.g., D.1, H.1.3, H.13.4).
- Attachments must not be embedded into the SSR, CAP or 45-day notification.

2.E.3 Encryption Requirements

The Office of Safeguards requires that all 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 minimum of 128-bit encryption key string
- Ensure a strong password or passphrase is generated to encrypt the file
- Communicate the password or passphrase 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 subject line and content of the email message will not be encrypted, so it is important that any sensitive information be contained in the attachment (encrypted document).

2.E.4 Safeguards Security Reports (SSR)

The SSR is the primary method for agencies to report to the IRS Office of Safeguards processes, procedures, and security and privacy controls in place to protect FTI in compliance with IRC § 6103(p)(4). Agencies have an annual requirement to submit SSRs after their initial receipt of FTI. There are enhanced requirements for agencies that are applying to receive FTI for the first time and for existing agencies requesting new FTI data streams.

2.E.4.1 Initial SSR Submission Instructions – New Agency Responsibilities

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

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

- Designate an agency Safeguards POC, see Section 1.5 Coordinating Safeguards Within an Agency
- Make program officials, contractors, and/or sub-contractors available to discuss access and use of FTI, as needed

The agency is required to submit evidentiary documentation for the controls shown in Table 3 in conjunction with the first submission of the agency's SSR.

Table 3 – SSR Evidentiary Documentation		
800-53 Control	**Control Name**	**Evidentiary Documents (Artifacts) for Review**
Section 2.C.5	Commingling and Labeling	• Screenshots of database schemas that will show electronic FTI labeling • Sample output (report/notice) that will show how FTI is labeled
AC-6	Least Privilege	• FTI data flow diagram (physical and logical) that will include all devices and inputs/outputs • Access Control Policy and Procedures
AC-17	Remote Access	• Screenshot of authentication screens
AC-20	Use of External Systems	• Access Control Policy and Procedures that will show the prohibition of using non-agency owned devices to access FTI and the FTI network
AU-2	Audit Events	• Audit and accountability policy and procedures for FTI information systems (e.g., network infrastructure, 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	Training Records	• Training material (for users and system security personnel) • Sample certification statement
CA-2	Assessments	• Independent Security Assessment Report (SAR) or other report reflecting the results of security testing, highlighting findings deemed "critical" or "high"
CA-5	Plan of Action and Milestones	• POA&M report that will show the completed risk mitigation activities and planned mitigation activities for identified weaknesses
CA-6	Authorization	• Documentation appointing the system Authorization Official • Signed Authority to Operate (ATO) for new systems (or DRAFT if ATO not yet granted)

Table 3 – SSR Evidentiary Documentation		
800-53 Control	**Control Name**	**Evidentiary Documents (Artifacts) for Review**
CM-8	System Component Inventory	• Complete listing of FTI inventory (includes networking devices, boundary protection devices and information system components) identifying: platform, operating system, and applicable software (e.g., DBMS, application development environments, web servers) • *Note*: The agency must provide sufficient version detail for each system component such that the Office of Safeguards can determine whether the system component is subject to receiving ongoing security support from the vendor
IA-2	Identification and Authentication (Organizational Users)	• Screenshots that will show the configuration of multifactor authentication solution(s) in place for all remote network access to systems containing FTI • Description of Authenticator Assurance Level implementation for public-facing systems displaying FTI
IA-5	Authenticator Management	• Password and Authenticator Management Policy and Procedures • Screenshots of local security policy for password management
IA-12	Identity Proofing	• Description of Identity Assurance Level (IAL) implementation for public-facing systems displaying FTI
IR-6	Incident Reporting	• Incident Response Plan and Procedures
MP-6	Media Sanitization	• Media Sanitization Policy and Procedures • Destruction log template
PE-3	Physical Access Control	• Physical Access Policy and Procedures • Alternative Worksite Policy and Procedures
PE-8	Visitor Access Records	• Sample visitor access log
PM-5	Inventory of Personally Identifiable Information	• Diagrams depicting the logical flow of FTI within the agency's network to include specific boundary protection, infrastructure devices and endpoints where FTI will be stored
PS-8	Personnel Sanctions	• Personnel Sanctions Policy and Procedures
RA-5	Vulnerability Scanning	• Vulnerability scanning Policy and Procedures

Table 3 – SSR Evidentiary Documentation		
800-53 Control	**Control Name**	**Evidentiary Documents (Artifacts) for Review**
SA-9	External Information System Services	• System and Services Acquisition Policy and/or Access Control Policy • Contracts with service providers containing Publication 1075 Exhibit 7 language
SC-4	Information in Shared System Resources	• System and Communication Policy and Procedures
SC-7	Boundary Protection	• Network architecture and design documents to include internet-facing network security components that will protect the FTI network
SC-8	Transmission Confidentiality and Integrity	• System and Communication Policy and Procedures • Network design diagram and documentation showing all FTI transmission protocols and encryption mechanisms identified
SI-2	Flaw Remediation	• Patch Management Policy and Procedure
SI-3	Malicious Code Protection	• Malicious Code Protection Policy and Procedure

If the agency does not submit all required evidentiary documentation as described above, the IRS reserves the right to conduct a safeguard review to assess the effectiveness of the controls established in order to approve the SSR prior to initial release of FTI. Subsequently, Safeguards will conduct a risk-based assessment to determine when to schedule an agency's first safeguard review after initial receipt of FTI.

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

2.E.4.2 Agencies Requesting New FTI Data Streams

Agencies currently receiving FTI with an approved SSR and seeking additional FTI data streams (i.e., FTI to be received under newly assigned program authority or expanded statutory authority under IRC § 6103), must submit the following documentation along with the request to receive the new data stream(s):

- Approved SSR for the most recent reporting period
- Current CAP with approved mitigation strategies for critical and significant findings
- Documentation of security testing for the system(s) where the new data stream will be processed. Any findings deemed "critical" must be mitigated
- A signed Authority to Operate (ATO) for the system(s) that will be receiving, processing, storing, accessing, protecting and/or transmitting the new FTI data stream that is not covered in the agency's SSR already on file

After the agency receives its new data stream, the subsequent SSR submission must reference the receipt of the new data stream and must describe all systems that receive, process, store, access, protect and/or transmit FTI. This SSR submission must also describe all security and privacy control implementations for the FTI environment(s).

2.E.4.3 Annual SSR Update Submission Instructions

The agency must update and submit the SSR annually. The purpose of the SSR is for agencies to document the implementation of security and privacy controls that impact the protection of FTI. Agencies must document significant changes to the environment, as applicable. Examples of changes include, but are not limited to:

- New data exchange agreements
- New computer equipment, systems or applications (hardware or software) (e.g., moving FTI systems to a FedRAMP authorized cloud environment, re-engineering legacy case management systems)
- New facilities including, office moves, new contractor or sub-contractor locations (e.g., print vendor, call center)
- Organizational changes, such as moving IT operations to a consolidated data center from an embedded IT operation
- Development of new business processes or procedures for handling FTI

The following information must be updated in each SSR submission to reflect routine updates or changes to the implementation of security and privacy controls and/or the agency's safeguarding program:

- Changes to information or procedures previously reported
- Current annual period safeguard activities (e.g., performing internal inspections, performing ongoing security and privacy control testing, providing security and privacy awareness training to employees)
- Planned actions affecting safeguard procedures (e.g., system upgrades, development of new policy framework, use of a new audit log monitoring solution)
- Agency use of contractors or sub-contractors (non-agency employees)

The annual SSR update must be submitted on the prior year's SSR analysis 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 and reduces the need for recreating the entire document.

2.E.4.4 SSR Submission Dates

The SSR must be submitted annually with all applicable attachments. Each submission of the SSR must include a description of updates or changes that have occurred during the reporting period.

Submission due dates are defined below:

Table 4 - SSR Submission 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
CO, CT, DC, DE, FL, GA, MP*	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

*The Postal abbreviation for Commonwealth of the Northern Mariana Islands was updated to MP.

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

When extenuating circumstances exist, agencies may request an SSR extension, in 30-day increments, with a maximum of 60 days. Extension requests must be submitted not later than 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 must be sent to the Office of Safeguards via SDT or sent via email to SafeguardReports@irs.gov, with the subject "SSR Extension Request". The body of the email must address the 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 five (5) business days after receipt of the request.

2.E.5 Corrective Action Plan

The Corrective Action Plan (CAP) is a report containing the findings, the recommended corrective actions, and targeted implementation dates for each weakness identified during an on-site, remote, or hybrid review. The CAP and SRR documents are the same in content, however, the CAP document has functionality to allow agencies to report their progress on corrective actions. The IRS will provide each agency an SRR along with a CAP upon completion of an on-site, remote or hybrid review. The agency

must complete the CAP by providing an updated status to each unresolved finding, including the projected or actual date to close the finding, as well as provide status updates to any remaining planned actions.

All findings must be addressed in a timely fashion or an out of cycle CAP review may be done to further address an agency's open critical and significant findings.

Safeguards will initiate communication with the agency's POC, and a formal engagement letter will be sent. At that time, the agency will be required to update their CAP and provide documentation for closure consideration of the remaining critical and significant findings. The out of cycle CAP review process will include:

- A preliminary discussion held prior to the review of the findings.
- During the review, the agency's CAP responses and supporting documentation will be addressed. Requests for additional information and clarification, including automated scanning reports, will be made by Safeguards.
- A closing conference will be held upon the completion of the agency's CAP review and a Preliminary Assessment Report (PAR) will be issued to provide the agency an overview of the findings addressed during the review.

The agency may be required to submit a mitigation plan if any critical findings remain open and escalation of the p7 process maybe initiated per Exhibit 3, USC Title 26, CFR § 301.6103(p)(7)-1.

The agency will receive an updated CAP to resolve outstanding issues in the next reporting cycle.

2.E.5.1 CAP Submission Instructions

The agency must update and submit the CAP semi-annually to document all corrective actions, taken or planned, in response to the findings enumerated in the SRR. To complete the CAP document, agencies must:

- Use the version sent by the Office of Safeguards with the SRR and must not alter the format
- Provide a written narrative in response to each finding
- Provide a planned implementation date or actual completion date in MM/DD/YYYY format for each finding response
- Provide evidentiary documentation to validate the closure of any findings identified as Critical or Significant
- Provide a signed certification from the Chief Information Security Officer (CISO) or Head of Agency to document and close findings that are no longer applicable to the agency's handling of FTI. Often, this occurs when agencies decommission systems that once transmitted FTI, replace applications or systems with newer technologies, or perform major upgrades to versions of systems that continue to receive, process, store, access, protect and/or transmit FTI.

2.E.5.2 CAP Submission Dates

CAP Submission due dates are defined below.

Table 5 – CAP Submission Dates		
	CAP with SSR	**CAP (only)**
Federal Agencies		
All Federal Agencies	January 31	July 31
State Agencies and Territories		
AK, AL, AR, AS, AZ, CA	February 28	August 31
CO, CT, DC, DE, FL, GA, MP*	March 31	September 30
GU, HI, IA, ID, IL, IN, KS	April 30	October 31
KY, LA, MA, MD, ME, MI	May 31	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

*The Postal abbreviation for Commonwealth of the Northern Mariana Islands was updated to MP.

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. Agency CAP submissions provided to the Office of Safeguards within 60 days of an upcoming review will be responded to as part of the review process.

When extenuating circumstances exist, agencies may request an extension for no more than 30 days. Extension requests must be submitted not later than 30 days prior to the scheduled CAP due date. Request for extensions will not be considered after the scheduled CAP due date. Extension requests must be sent to the Office of Safeguards via SDT or sent via email to SafeguardReports@irs.gov, with the subject "CAP Extension Request". The body of the email must address the 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 five (5) business days after receipt of the request.

2.E.6 Notification Reporting Requirements

IRC § 6103 limits the usage of FTI to only those purposes explicitly stated. Due to the security and privacy 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 of at least 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 1.1), the following circumstances or technology implementations require the agency to submit notification to the Office of Safeguards via the SafeguardReports@irs.gov, mailbox, a minimum of 45 days ahead of the planned implementation:

Table 6 – Notification Reporting

Prior to…	Requirement
Implementing Cloud Computing	Submit Notification
Disclosure to a Contractor	Submit Notification
Re-disclosure by Contractor to Sub-Contractor	Submit Notification and receive approval
Using FTI in Tax Modeling for Tax Administration	Submit Notification and receive approval
Using FTI in Pre-Production Environment	Submit Notification and receive approval

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

2.E.6.1 Cloud Computing

Receiving, processing, storing, accessing, protecting, and/or transmitting FTI in a cloud environment requires prior notification to the Office of Safeguards.

The intent of the notification is to require agencies to:

- Document the physical locations where FTI will be processed to ensure FTI remains onshore
- Document the cloud service provider's FedRAMP authorization such that Safeguards does not have the responsibility to assess the physical security of cloud service provider facilities
- Explain how encryption will be used to prevent unauthorized disclosures to cloud service provider employees
- Document all agency-managed security and privacy controls

If the agency cannot demonstrate it prevents the cloud service provider from having logical access to the data, the agency must submit a notification for disclosure to a contractor or sub-contractor.

Refer to Section 3.3.1, Cloud Computing and the Safeguards website for more information related to cloud computing requirements.

2.E.6.2 Contractor or Sub-Contractor Access

Redisclosure of FTI to contractors or sub-contractors by authorized agencies requires notification to IRS at least 45 days prior to the planned re-disclosure. Contractors or sub-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 sub-contractor services. Approval is required if the (prime) contractor hires additional sub-contractor services in accordance with Exhibit 6, Contractor 45-Day Notification Procedures.

Notification is also required for contractors or sub-contractors to perform statistical analysis, tax modeling or revenue projections (see Section 1.4, State Tax Agency Limitations).

2.E.6.3 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 and Disclosure for approval of the modeling methodology (see Section 1.4, State Tax Agency Limitations).

Tax modeling approvals are valid up to three years. If the agency needs to continue the use of FTI in tax modeling past the approved timeframe, a new request must be submitted to the Office of Safeguards.

2.E.6.4 Live Data Testing

Agencies must submit a Data Testing Request (DTR) form to request approval to use live FTI in a testing environment. The intent of the notification is to ensure agencies do not process FTI in environments that do not have the same security and privacy controls as the production environment. Safeguards must review the security posture of the development or test environment as described in the agency's notification document submission to determine whether the agency has reduced the risk to an acceptable level.

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. State taxing agencies must ensure their Need and Use Justification statements include the use of FTI in a test environment.

Testing request approvals are valid up to three years from the date of the approval. If testing FTI data is no longer required before the approval expires, FTI must be removed from the test environment. If the agency needs to continue the use of FTI in pre-production testing activities past the approved timeframe, a new request for live data must be submitted to the Office of Safeguards.

Please see the Office of Safeguards website for additional information.

2.F Disposing of FTI – IRC § 6103(p)(4)(F)

2.F.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 will either return the information (including any copies made) to the office from which it was originally obtained or destroy the FTI. Agencies will include a

description of the procedures implemented in their annual SSR. See Section 2.E, Reporting Requirements - 6103(p)(4)(E) for additional reporting requirements.

2.F.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 2.B.4, FTI in Transit).

2.F.3 Destruction and Disposal

FTI furnished to the user and any paper material generated from it, 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 paper FTI:

Table 7 - 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 crosscut shredders that 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 NIST Control MP-6, 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 Section 2.F.3.1, Media Sanitation).

- Destroy microforms (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 NIST Control MP-6, Media Sanitization and Section 2.F.3.1, 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.

2.F.3.1 Media Sanitization

The type of sanitization performed depends on whether or not the media will be reused by the agency or 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 must be selected as the sanitization method. If the media will not be reused at all, then destruction is the method for media sanitization. The requirements are applicable for media used in "pre-production" or "test" environments. The technique for clearing, purging, and destroying media depends on the type of media being sanitized.

The following media sanitization requirements are required:

- Every third piece of media must be tested after sanitization has been completed.
- Media sanitization must be witnessed or verified by an agency employee.
- 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.

See also MP-6. Media Sanitization. Additional media sanitization requirements are available on the Office of Safeguards website.

2.F.4 Other Precautions

FTI must never be disclosed to an agency's agents, contractors, or sub-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 or sub-contractor.

If a contractor or sub-contractor is used:

- The contract must contain safeguard language in Exhibit 7a and 7b, Safeguarding Contract Language as appropriate to the contract to ensure the protection of FTI.
- Destruction of FTI must be certified by the contractor or sub-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 or sub-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, the agency must annually validate and maintain the most recent copy of the NAID certification.

3.0 CYBERSECURITY REQUIREMENTS

3.1 General

This section details the information technology (IT) security and privacy requirements agencies must meet to adequately protect FTI under their administrative control. While the Office of Safeguards has the responsibility to ensure the protection of FTI, it is the responsibility of the agency to implement effective security and privacy controls into its own IT infrastructure.

Section 4.0, NIST 800-53 Security and Privacy Controls, contains a catalog of technical and nontechnical security and privacy control requirements that must be implemented to protect electronic FTI. These requirements apply to 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. Selected controls are defined using guidelines specified in the latest version of NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, and in IRS directives.

3.2 Assessment Process

The Office of Safeguards will assess agency compliance with the security and privacy requirements identified in this publication as part of the annual reporting and review processes. The IT assessment will include a review of the agency's FTI inventory. All IT systems and supporting components receiving, accessing, storing, processing, protecting, or transmitting FTI must be included in the agency's FTI inventory. This includes, for example: end user and administrator workstations, host operating system(s), contractor systems or laptops, web servers, database management systems, hypervisors, storage arrays and cloud environments. The FTI inventory must also include networking components used to protect or transmit FTI and access an FTI environment. This includes, for example: border/perimeter firewall, virtual private network (VPN), core routers, wireless networks, voice over IP systems and site to site endpoints established with external networks when FTI is shared and/or accessed outside of the LAN.

The scope of assessments includes any technology used to receive, process, store, access, protect and/or transmit FTI that is owned and managed by 1) the agency, 2) a state's consolidated IT organization, 3) the agency's contractors and sub-contractors (e.g., print vendors, collections agencies, application development contractors, network engineers at a state consolidated IT office, etc.) and 4) the agency's constituent counties included in an assessment.

Requirements are assessed using manual and automated assessment procedures as they relate to NIST SP 800-53 security and privacy controls as outlined in this publication. To ensure a standardized cybersecurity review process, Cybersecurity Reviewers will conduct assessments using Safeguards Computer Security Evaluation Matrices (SCSEM) to evaluate agency policies, procedures and IT systems that receive, process, store, access, protect and/or transmit FTI. The following techniques will be used to collect evidence required to complete SCSEM assessments:

Table 8 – Assessment Methodologies

Testing Technique	Description
Automated Compliance Assessment Testing	Cybersecurity Reviewers will use compliance 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 laptop computers or when applicable, agency software instances compatible with IRS testing software. Automated testing must be performed using IRS Safeguards-specific audit profiles that are available on the Office of Safeguards website.
Manual Security and Privacy Control Testing	Cybersecurity Reviewer manual test methods will include interviews and examination of documentation and onscreen configuration settings.

Please see Section 1.6.2, During the Review for information on the review process.

3.3 Technology-Specific Requirements

3.3.1 Cloud Computing

To use a cloud computing model to receive, process, store, access, protect and/or transmit FTI, the agency must comply with all requirements in this publication. The following mandatory requirements are in effect for using cloud services to receive, process, store, access, protect and/or transmit FTI:

a. FedRAMP Authorization: FTI may only be introduced to cloud environments that have been provided an authorization by the Joint Advisory Board (JAB) or a Federal Agency.

b. Onshore Access: Agencies must leverage vendors and services where (i) all FTI physically resides in systems located within the United States; and (ii) all accesses, and support of the systems and services are performed from the United States, its possessions and territories.

c. Physical Description: Agencies and their cloud providers must provide a complete listing of all data center addresses where FTI will be received, processed, stored, accessed, protected and/or transmitted in their 45-Day notification form.

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 certified and operate utilizing the latest FIPS 140 compliant module(s). This requirement must be included in the SLA.

e. Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA.

   Supplemental Guidance: If the agency is able to encrypt data in transit and at rest using the latest FIPS 140 certified solutions and maintain sole ownership of encryption keys, preventing logical access from the cloud service providers, Safeguards will consider this a logical barrier and will allow data types with restrictions (e.g., IRC § 6103 (l)(7) data) to move to a cloud environment. Using FIPS 140 certified encryption at rest exempts third-party contractors from some protection requirements such as training and background investigation requirements.

f. 45-Day Notification: The agency must notify the IRS Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment, per Section 2.E.6, Notification Reporting Requirements.

g. Service Level Agreements and Contracts: The agency must establish security and privacy controls, based on IRS Publication 1075, for how FTI is received, processed, stored, accessed, protected and/or transmitted inside the cloud environment. Agencies must provide the requirements through a legally binding contract or SLA with their third-party cloud provider.

h. Data Isolation: Software and/or services that receive, transmit, process or store 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.

i. Risk Assessment: The agency must conduct an annual assessment of the security and privacy controls in place on all information systems used for receiving, processing, storing, accessing, protecting and/or transmitting FTI.

j. Persistence of Data in Relieved Assets: Storage devices where FTI has resided must be securely sanitized and/or destroyed using methods acceptable by NIST. This requirement must be included in the SLA.

k. Multifactor Authentication: Agencies must implement sufficient multifactor authentication when their cloud solutions are available from the internet (i.e., there is access to the cloud solution from outside of the agency's trusted network). If the cloud can only be accessed from an agency's internal network, multifactor authentication must be implemented by agency solution(s) when establishing a remote connection.

l. Security Control Implementation: Customer defined security and privacy controls must be identified, documented and implemented, and must comply with Publication 1075 requirements.

Supplemental Guidance: If the agency or system has the ability to automatically provision or deprovision resources based on need, then it is considered a cloud environment. The service and deployment model used in a cloud computing environment will determine the responsibility for security and privacy controls implementation between the agency and the cloud provider for the protection of FTI that is stored or processed in the cloud environment. The Office of Safeguards tailors its assessment of an agency's cloud solution based on the cloud vendor's FedRAMP authorization boundary. For systems where cloud service providers maintain complete control over and have documented the security and privacy controls of those systems in its FedRAMP authorization framework, the Office of Safeguards will assess those controls using the Cloud SCSEM. For agency-managed systems that reside logically in the cloud environment, but remain outside of the FedRAMP authorization boundary, the Office of Safeguards will leverage its SCSEMs to assess the security posture of those systems. All testing will be performed using the methods described in Section 3.2, Table 8, Assessment Methodologies.

Additional cloud computing guidance is available on the Office of Safeguards website.

To determine if your agency is utilizing a cloud please use the following Cloud Decision Tree

Note: https://www.irs.gov/pub/irs-utl/cloud-decision-tree.pdf

3.3.2 Email Communications

If the agency determines FTI is not permitted to be included in email, a written policy must be established and distributed to:

a. Prohibit FTI in email transmissions; and

b. Clearly state the actions that will be taken if FTI is inadvertently sent in email.

If the agency determines FTI is permitted to be included in email, a written policy must be established and distributed to:

a. Prohibit FTI in email transmissions outside of the agency's internal network;

b. Ensure transmissions are sent only to authorized recipients; and

c. Require adequate labeling (e.g., email subject contains “FTI”) and protection.

Additionally, the agency must ensure FTI is properly protected and secured when being transmitted via email. At a minimum:

a. Mail servers and clients must be securely configured. Underlying operating systems of on-premises mail servers must be hardened and included in the agency's FTI inventory. A 45-day cloud notification must be submitted for cloud-hosted mail solutions.

b. The network infrastructure must be securely configured to block unauthorized traffic, limit security vulnerabilities, and provide an additional security layer to an agency’s mail servers and clients.

c. Audit logging must be implemented to track all sent and received emails containing FTI.

d. Email transmissions containing FTI must be encrypted using the latest FIPS 140 validated mechanism.

e. 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.

3.3.3 Facsimile and Facsimile Devices

If the agency determines FTI is not permitted to be included in fax communications, a written policy must be established and distributed to:

a. Prohibit FTI in fax communications; and

b. Clearly state the actions that will be taken if FTI is inadvertently faxed.

If the agency determines FTI is permitted to be included in fax communications, a written policy must be established and distributed to ensure fax communications are transmitted 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, that 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 via collect call, if necessary, to report the disclosure and confirm destruction of the information

Additionally, the agency must ensure facsimile devices used to transmit FTI are properly protected and secured. At a minimum:

a. When applicable, encrypt information or be connected to a secure network

b. Securely configure multifunction devices (MFD) used to receive or transmit fax communications

If digital fax servers are used, they should be hardened like other servers containing FTI.

3.3.4 Mobile Devices

To use FTI in a mobile device environment, the agency must implement a centralized mobile device management (MDM) solution to authenticate and manage the configuration of agency-owned and personally owned mobile devices prior to allowing access to the internal network. Further guidance of the configuration of mobile device solutions can be found on the Office of Safeguards website.

See also AC-19: Access Control for Mobile Devices.

3.3.5 Multifunction Devices (MFDs) and High-Volume Printers (HVPs)

If the agency determines FTI is not permitted to be printed, a written policy must be established and distributed to:

a. Prohibit FTI from being printed

b. Clearly state the actions that will be taken if FTI is inadvertently printed

If the agency determines FTI is permitted to be printed, a written policy must be established and distributed to:

a. Prohibit printing FTI to printers outside of the agency's internal network

b. Ensure printed FTI is sent only to authorized printers (e.g., multifunction devices, standalone printers, high-volume printers)

c. Require adequate labeling and protection of all printed FTI

Additionally, the agency must ensure MFDs and HVPs are configured securely and included in the agency's FTI inventory.

3.3.6 Network Boundary and Infrastructure

Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. 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). Inbound services shall be prohibited unless a valid business case can establish their necessity. All remote access must be routed and monitored through a managed solution and accomplished using multifactor authentication per the requirements of NIST Control IA-2, Identification and Authentication (Organizational Users). FTI end users and privileged administrators may access the FTI environment over a secured wireless local area network (WLAN) infrastructure that complies with the Institute of Electrical and Electronic Engineers (IEEE) 802.11i wireless security standard and uses WPA2-certified equipment and software.

All networking devices responsible for protecting the FTI environment or used to access the FTI environment must be included in the agency's FTI inventory.

Additional network protection requirements are available on the Office of Safeguards website.

3.3.7 Virtual Desktop Infrastructure

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. Using VDI environments is the only manner in which agencies may authorize their users to leverage personally owned devices to access and/or manage information systems that receive, process, store, access, protect and/or transmit FTI.

See AC-20, Use of External Systems and the IRS Office of Safeguards website for more information.

3.3.8 Public-Facing Systems

FTI is considered nonpublic information and may never be posted or shared on an unauthenticated publicly accessible system (e.g., public website). Agencies may have business needs to provide FTI to its individual constituents, customers, clients and/or stakeholders using interactive applications. Examples of such systems include tax applications meant to provide account information to taxpayers or practitioners, state-based marketplace systems, child support online portals, etc. Publicly facing systems are typically internet-based applications but may also include interactive voice response technology.

Should an agency choose to provide FTI through a publicly facing system, it must implement the following requirements:

a. The system architecture is configured as a multi-tier architecture with physically and/or logically separate systems that provide layered security of the FTI. Access to FTI in a back-end database must be brokered through multiple layers such that a public user cannot query the database directly.

b. Each individual technology (e.g., application server, web server software, firewall) within the system architecture that receives, processes, stores, accesses, protects and/or transmits FTI is hardened in accordance with the requirements in this publication, the appropriate SCSEM and is subject to the agency's security testing capability.

c. Access to FTI via the system must only occur when following strong identity proofing and authentication processes consistent with the latest guidance in NIST SP 800-63-3, *Digital Identity Guidelines* and the other documents in the 800-63 suite: NIST SP 800-63A, *Enrollment and Identity Proofing*, NIST SP 800-63B, *Authentication and Lifecycle Management and* NIST SP800-63C, *Federation and Assurances*. Consistent with choosing a moderate-level baseline for security controls, the Office of Safeguards has determined that public-facing systems must implement Identity Assurance Level (IAL) 2 to confirm the identity at the point an account is established and then must use Authentication Assurance Level (AAL) 2 to confirm the veracity of the account's use upon each user login. Agencies may use Federation Assurance Level (FAL) 2 should they leverage federated identities.

   IAL2: There is evidence that supports the real-world existence of the claimed identity and the evidence verifies that the applicant is appropriately associated with this real-world identity. Either remote or physical identity proofing may be used depending on the evidence provided during the identity proofing step.

   AAL2: There is a high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is

required through secure authentication protocols. Approved cryptographic techniques are required.

FAL2: There is a need to use federated identities to leverage sufficient encryption such that the agency is 1) the only party capable of decrypting the assertion from the third-party identity provider and 2) the identity provider cryptographically signs the assertion.

4.0 NIST 800-53 SECURITY AND PRIVACY CONTROLS

Section 4.0, NIST SP 800-53 Control Requirements, provides the security and privacy control requirements that relate to protecting FTI. Selected controls are based on the moderate security baseline defined by NIST and have been tailored based on the integration of privacy control requirements and those controls required to protect the confidentiality of FTI.

Where applicable, the Office of Safeguards has included NIST control enhancements, IRS and Treasury defined requirements to protect the confidentiality of FTI. NIST control enhancements are identified with a CE designation. IRS and Treasury defined requirements are identified as *IRS-Defined.*

4.1 ACCESS CONTROL

AC-1 Access Control Policy and Procedures

a. Develop, document, and disseminate to **designated agency personnel**:

   1. An agency or organization-level access control policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the access control policy and associated access controls;

b. Designate an **agency official** to manage the access control policy and procedures

c. Review and update the current access control

   1. Policy **every three (3) years (or if there is a significant change)**; and

   2. Procedures **every three (3) years (or if there is a significant change)**.

AC-2 Account Management

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require conditions for group and role membership;

d. Specify:

   1. Authorized users of the system;

   2. Group and role membership; and

   3. Access authorizations (i.e., privileges) and other attributes (as required) for each account.

e. Require approvals by **the system owner or designated representative** for requests to create accounts;

f. Create, enable, modify, disable and remove accounts in accordance with **agency account management procedures prerequisites;**

g. Monitor the use of accounts;

h. Notify account managers and designated agency official within:

    1. 24 hours when accounts are no longer required;

    2. 24 hours when users are terminated or transferred; and

    3. 24 hours when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

    1. A valid access authorization;

    2. Intended system usage; and

    3. Under the authority to re-disclosed FTI under the provisions of IRC § 6103;

j. Review accounts for compliance with account management requirements **annually for user account and semi-annually for privileged accounts;**

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

Control Enhancements:

(CE-1) Automated System Account Management: Support the management of system accounts using automated mechanisms.

Supplemental Guidance: Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

(CE-2): Removal of Temporary and Emergency Accounts: Automatically **disable and remove** temporary and emergency accounts after **two (2) business** days.

(CE-3): Disable Accounts: Disable accounts within 120 days when the accounts:

a. Have expired;

b. Are no longer associated to a user or individual;

c. Are in violation of organizational policy; or

d. Have been inactive for 120 days for non-privileged accounts and 60 days for privileged accounts

(CE-4) Automated Audit Actions: Automatically audit account creation, modification, enabling, disabling and removal actions.

(CE-7) Privileged User Accounts:

a. Establish and administer privileged user accounts in accordance with a role-based access scheme; an attribute-based access scheme

b. Monitor privileged role or attribute assignments;

c. Monitor changes to roles or attributes; and

d. Revoke access when privileged role or attribute assignments are no longer appropriate.

(CE-9): Restrictions on Use of Shared and Group Accounts: Only permit the use of shared and group accounts that meet agency-defined conditions for establishing shared and group accounts.

Supplemental Guidance: Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts. This includes service accounts that can be used for computer logon by a user (e.g., interactive logon is not disabled).

(CE-12) Account Monitoring for Atypical Usage:

a. Monitor system accounts for agency-defined atypical usage; and

b. Report atypical usage of system accounts to agency-defined personnel or roles.

Supplemental Guidance: Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals.

(CE-13): Disable Accounts for High-Risk Individual: Disable accounts of users posing a significant risk within **one (1) day** of discovery of the risk.

Supplemental Guidance: Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes the potential adverse impacts to organizational operations and assets, individuals, other organizations, the state, or the Nation. Close coordination and cooperation among authorizing officials, system administrators and human resource managers is essential for timely execution of this control enhancement.

AC-3 Access Enforcement

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

(IRS-Defined): Users having accounts with administrator access privileges may access those accounts only from agency-owned or authorized contractor systems.

Supplemental Guidance: A key intent is to prohibit personally-owned or public kiosk (e.g., library) systems from being used for remote administrator access. If individuals with administrator rights require email or Internet access beyond local boundaries, one alternative would be to issue separate, non-privileged accounts (one per affected individual) for that purpose. For the considerations of this section, administrator accounts/rights are those that allow for the installation or configuration of software on agency assets receiving, processing, storing, accessing, protecting and/or transmitting FTI.

Control Enhancements:

(CE-9) Controlled Release: Release information outside of the system only if:

a. The receiving system accessing, processing, storing, or transmitting FTI provides Publication 1075 required protections; and

b. Agency-defined controls, Publication 1075 requirements, FedRAMP ATO are used to validate the appropriateness of the information designated for release.

(CE-11) Restrict Access to Specific Information Types: Restrict access to data repositories containing Federal Tax Information.

AC-4 Information Flow Enforcement

Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based **on the technical safeguards in place to protect Federal Tax Information (FTI).**

Additional requirements for protecting the flow of FTI can be found in Section 3.3, Technology-Specific Requirements.

AC-5 Separation of Duties

a. Identify and document separate duties of individuals to prevent harmful activity without collusion; and

b. Define system access authorizations to support separation of duties.

AC-6 Least Privilege

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 organizational tasks.

Control Enhancements:

(CE-1): Authorize Access to Security Functions: Authorize Access for Security Functions to:

a. Explicitly authorize access to security functions deployed in hardware, software, and firmware; and

b. Security-relevant information.

(CE-2): Non-Privileged Access for Nonsecurity Functions: Require that users of system accounts or roles with access to security functions including but not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited and setting intrusion detection parameters use non-privileged accounts or roles, when accessing nonsecurity functions.

(IRS-Defined): Prohibit accounts with administrative privileges (including local administrator rights) from web browsing and other Internet connections outside of the local protected boundary unless such risk is accepted in writing by the agency's CISO.

(IRS-Defined): Block accounts with administrative privileges (including local administrator rights) from access to email unless such risk is accepted in writing by the agency's CISO.

(CE-6): Privileged Access by Non-Organizational Users: Prohibit privileged access to the system by non-organizational users.

(CE-7): Review of User Privileges

a. Review **annually** the privileges assigned to **FTI** to validate the need for such privileges; and

b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

(CE-8): Privilege Levels for Code Execution: Prevent the following software from executing at higher privilege levels than users executing the software: agency-defined software.

Supplemental Guidance: This item should be tracked on the agency's POA&M.

(CE-9): Auditing Use of Privileged Functions: Audit the execution of privileged functions.

(CE-10): Prohibit Non-privileged Users from Executing Privileged Functions: Prevent non-privileged users from executing privileged functions.

Supplemental Guidance: If individuals with administrator rights require email or Internet access beyond local boundaries, one alternative would be to issue separate, non-privileged accounts (one per affected individual) for that purpose. For the considerations of this section, administrator accounts/rights are those that allow for the installation or configuration of software on any agency assets receiving, processing, storing, accessing, protecting and/or transmitting FTI.

Supplemental Guidance: If individuals with administrator rights require email or Internet access beyond local boundaries, one alternative would be to issue separate, non-privileged accounts (one per affected individual) for that purpose. For the considerations of this section, administrator accounts/rights are those that allow for the installation or configuration of software on any agency assets storing, processing, transmitting, or protecting FTI.

AC-7: Unsuccessful Logon Attempts

a. Enforce a limit of **three (3) consecutive** invalid logon attempts by a user during a **120-minute** period; and

b. Automatically lock the account for **15 minutes** or until **released by an administrator** when the maximum number of unsuccessful attempts is exceeded.

Control Enhancements:

(CE-2): Purge or Wipe Mobile Device: Purge or wipe information from mobile devices based on agency-defined purging or wiping requirements and techniques after **ten (10) consecutive**, unsuccessful device logon attempts.

Supplemental Guidance: This control enhancement applies only to mobile devices for which a logon occurs. The logon is to the mobile device, not to any one account on the device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.

AC-8: System Use Notification

a. Display a warning banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

    1. Users are accessing a U.S. Government System;

    2. System usage may be monitored, recorded, and subject to audit;

    3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

    4. Use of the system indicates consent to monitoring and recording;

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

c. For publicly accessible systems:

    1. Display system use information warning banner before granting further access to the publicly accessible system;

    2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities and

    3. Include a description of the authorized uses of the system.

Supplemental Guidance: 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.

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

AC-11: Device Lock

a. Prevent further access to the system by initiating a device lock after **15 minutes** of inactivity; requiring the user to initiate a device lock before leaving the system unattended; and

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks are implemented where session activities can be determined. This is typically at the operating system level but can also be at the application level. Device locks are not an acceptable substitute for logging out of systems, for example, if organizations require users to log out at the end of workdays.

Control Enhancements:

(CE-1): Pattern-Hiding Displays: Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Supplemental Guidance: The pattern-hiding display can include static or dynamic images, for example,

patterns used with screen savers, photographic images, solid colors, clock, battery life indicator or a blank screen, with the caveat that controlled unclassified information is not displayed.

AC-12: Session Termination

Automatically terminate a user session after **30 minutes of inactivity.**

Supplemental Guidance: 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 agency system. Such user sessions can be terminated without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on system use.

Control Enhancements:

(CE-1): User-Initiated Logouts: Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to systems accessing, processing, storing, or transmitting FTI.

AC-14: Permitted Actions Without Identification or Authentication

a. Identify specific user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Supplemental Guidance: This control addresses situations in which agencies determine that no identification or authentication is required in agency systems. Agencies may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites. Access to FTI without identification and authentication is strictly prohibited.

AC-17: Remote Access

a. Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

Supplemental Guidance: Remote access is access to agency systems (or processes acting on behalf of users) communicating through external networks such as the Internet. Remote access methods include, for example, dial-up, broadband, and wireless. Remote access controls apply to systems other than public web servers or systems designed for public access. Any remote access where (i) FTI is accessed or (ii) an FTI environment is administered over the remote connection must be performed using multifactor authentication. Requirements of multifactor authentication are provided in NIST Control IA-2: Identification and Authentication (Organizational Users).

Control Enhancements:

(CE-1): Monitoring and Control: Employ automated mechanisms to monitor and control remote access methods.

(CE-2): Protection of Confidentiality and Integrity Using Encryption: Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

(CE-3): Managed Access Control Points: Route remote accesses through authorized and managed network access control points.

(CE-4): Privileged Commands and Access

a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: compelling operational needs defined by the agency; and

b. Document the rationale for remote access in the security plan for the system.

Supplemental Guidance: Rationale must be documented in agency's SSR as it relates to the FTI environment.

(CE-9): Disconnect or Disable Access: Provide the capability to disconnect or disable remote access to the system within agency-defined time period.

AC-18: Wireless Access

1. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

2. Authorize each type of wireless access to the system prior to allowing such connections.

Control Enhancements:

(CE-1): Authentication and Encryption: Protect wireless access to the system using authentication of both users and devices and encryption.

(CE-3): Disable Wireless Networking: Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

Supplemental Guidance: Disable (through automated means, where technically possible) unapproved wireless networking capabilities of desktops, laptops, printers, copiers, fax machines, SCADA systems and other devices; and monitor through automated means for unauthorized changes. One alternative yet acceptable approach to “monitoring through automated means” is regularly pushing out settings that restrict unapproved wireless connections.

(IRS-Defined): Guest wireless networks operated by or on behalf of the agency, data center or vendor managed facilities must be completely logically separate from all other secured internal networks.

(IRS-Defined): Monitor for unauthorized wireless access to the information system and enforce requirements for wireless connections to the information system.

(IRS-Defined): Employ security mechanisms for wireless networks consistent with the sensitivity of the information to be transmitted. FIPS 140 validated encryption must be employed in all wireless networks used to access FTI and/or manage an FTI environment.

(IRS-Defined): Perform both attack monitoring and vulnerability monitoring on the wireless network to support WLAN security.

Additional requirements for protecting FTI on wireless networks are provided in Section 3.3.6, Network Boundary and Infrastructure.

AC-19: Access Control for Mobile Devices

a. Establish configuration requirements, connection requirements and implementation guidance for organization-controlled mobile devices to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

Supplemental Guidance: A mobile device is considered a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device requirements are not applicable to laptop computers.

Control Enhancements:

(CE-5): Full Device and Container-Based Encryption: Employ full-device encryption using the latest FIPS 140 validated encryption on areas where FTI resides to protect the confidentiality and integrity of information on agency-owned mobile devices and mobile devices that are part of a BYOD implementation. POA&M findings must be documented and tracked when no such encryption technology solutions are available to address a specific device,

Additional requirements on protecting FTI accessed by mobile devices are provided in Section 3.3.4, Mobile Devices, Section 2.C.7, Offshore Operations and on the Office of Safeguards website.

AC-20: Use of External Systems

a. Establish terms and conditions, consistent with the trust relationships established with other organizations owning, operating and/or maintaining external systems, allowing authorized individuals to:

    1. Access the system from external systems; and

    2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of non-agency managed external systems.

Supplemental Guidance: External information systems, or non-agency-owned equipment, include any technology used to receive, process, store, access, protect and/or transmit FTI that is not owned and managed by 1) the agency or the agency-run mobile device management system, 2) a state's consolidated IT office, 3) one of the agency's approved contractors or sub-contractors (e.g., print vendors, collections agencies, application development contractors, network engineers at a state consolidated IT office, etc.) or 4) one of the agency's constituent counties. To ensure a third-party contractor system is not considered an external information system, the agency must include Exhibit 7 language in its contract with the service provider. Examples of external information systems include but are not limited to: 1)

personally-owned devices, which includes any device owned by an individual employee, rather than the agency itself; and 2) devices owned and managed by agency stakeholders that do not have proper approvals to receive, process, store, access, protect and/or transmit FTI.

Control Enhancements:

(CE-2): Portable Storage Devices - Restricted Use: Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using organizational-defined policy.

(CE-3): Non-Organizationally Owned Systems and Components - Restricted Use: Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using Publication 1075 requirements.

Supplemental Guidance: The IRS Office of Safeguards allows connections from external information systems only in the event the agency has configured a virtual desktop infrastructure (VDI) solution to receive, secure and manage remote connections.

(*IRS-Defined*): Approval by the agency CISO is required for connection of non-government furnished or contractor-owned IT devices (including USB-connected portable storage and mobile devices) to agency-owned systems or networks receiving, processing, storing, accessing, protecting and/or transmitting FTI. This requirement does not apply to networks and systems intended for use by the general public.

Additional VDI requirements are provided in Section 3.3.7, Virtual Desktop Infrastructure and on the Office of Safeguards website.

(CE-5): Portable Storage Devices - Prohibited Use: Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.

AC-21: Information Sharing

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and **use restrictions for information sharing circumstances where user discretion is required and permitted by IRC § 6103**; and

b. Employ **automated mechanisms or manual processes compliant with IRC § 6103** to assist users in making information sharing and collaboration decisions.

Supplemental Guidance: 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.

AC-22: Publicly Accessible Content

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information at a **minimum quarterly** and remove such information, if discovered.

Supplemental Guidance: FTI is considered nonpublic information and may never be posted or shared on a publicly accessible system.

AC-23: Data Mining Protection

Employ agency-defined data mining prevention and detection techniques for agency-defined data storage objects to detect and protect against unauthorized data mining.

4.2 AWARENESS AND TRAINING

AT-1: Awareness and Training Policy and Procedures

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

    1. An agency or organization-level security and privacy and awareness and training policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the awareness training policy and procedures; and

c. Review and update the current awareness and training:

    1. Policy **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

AT-2: Awareness Training

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

    1. As part of initial training for new users and annually thereafter; and

    2. When required by system changes or following assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;

b. Employ the following techniques to increase the security and privacy awareness of system users by providing one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training.

c. Update literacy training and awareness content annually and following system changes and

d. Incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques.

Control Enhancements:

(CE-1): Practical Exercises: Provide practical exercises in literacy training that simulate events and incidents.

Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering

attempts to collect information, gain unauthorized access or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Privacy-related practical exercises may include, for example, practice modules with quizzes on handling personally identifiable information and affected individuals in various scenarios.

(CE-2): Insider Threat: Provide literacy training on recognizing and reporting potential indicators of insider threat.

Supplemental Guidance: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence and other serious violations of organizational policies, procedures, directives, rules or practices. Security and privacy awareness training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through organizational channels in accordance with established policies and procedures.

(CE-3): Social Engineering and Mining: Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Supplemental Guidance: Social engineering is an attempt to trick someone into revealing information or taking an action that can be used to attack or compromise systems. Examples of social engineering include phishing, pretexting, baiting, quid pro quo, and tailgating. Social mining is an attempt, in a social setting, to gather information about the organization that may support future attacks. Security and privacy awareness training includes information on how to communicate concerns of employees and management regarding potential and actual instances of social engineering and mining through organizational channels based on established policies and procedures.

Treasury Directive: Train users and provide means to ensure workstations are adequately protected from theft, particularly regarding laptops acting as workstations.

(IRS-Defined): Distribute security and privacy awareness reminders/updates to all users on at least a quarterly basis.

Supplemental Guidance: This is in addition to annual awareness training. Security awareness updates may be sent via email. Unlike the need to track annual training by individual, agencies are not required to track quarterly awareness updates by individual.

(IRS-Defined): Conduct phishing email simulation exercises on at least a quarterly basis.

(CE-4): Suspicious Communications and Anomalous System Behavior: Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using agency-defined indicators of malicious code

AT-3: Role-Based Training

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: information system security manager (ISSM); information system security officer (ISSO); security specialist; system and software developers; system, network and database administrators; programmer/systems analyst; and personnel having access to FTI

    1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and

    2. When required by system changes;

b. Update role-based training content annually and following system changes and Update literacy training and awareness content annually and following system changes; and

c. Incorporate lessons learned from internal or external security or privacy incidents into role-based training.

Supplemental Guidance: Agencies may determine the appropriate content of security and privacy training based on the assigned roles and responsibilities of individuals and the specific security and privacy requirements of organizations and the systems to which personnel have authorized access, including security-related technical training specifically tailored for assigned duties. Additional roles that may require role-based security and privacy training include, for example, system owners; authorizing officials; system security officers; privacy officers; enterprise architects; acquisition and procurement officials; systems engineers; personnel conducting configuration management activities; personnel performing verification and validation activities; auditors; personnel having access to system-level software; security and privacy control assessors; personnel with contingency planning and incident response duties; and personnel with privacy management responsibilities.

AT-4: Training Records

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for a **period of five (5) years.**

AT-6: Training Feedback

Provide feedback on organizational training results to the following personnel: Agency Senior Management and Agency Disclosure Personnel on an annual basis.

4.3 AUDIT AND ACCOUNTABILITY

AU-1: Audit and Accountability Policy and Procedures

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

   1. An agency or organization-level audit and accountability policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

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

b. Designate an agency official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:

   1. Policy **every three (3) years (or if there is a significant change)**; and

   2. Procedures **every three (3) years (or if there is a significant change)**.

AU-2: Audit Events

a. Identify the types of events that the system is capable of logging in support of the audit function:

   1. All accesses or attempts to access an FTI system, including the identity of each user and device;
   2. Logoff activities;
   3. Activities that might modify, bypass, or negate IT security safeguards;
   4. Security-relevant actions associated with processing FTI;
   5. User generation of reports and extracts containing FTI;
   6. Any interaction with FTI through an application;
   7. Password changes;
   8. Creation or modification of groups;
   9. Privileged user actions;
   10. Access to the system;
   11. Creating and deleting files;
   12. Change of permissions or privileges;
   13. Command line changes and queries;
   14. Changes made to an application or database;
   15. System and data interactions;
   16. Opening and/or closing of files; and
   17. Program execution activities.

b. Coordinate the event logging function with other organizational entities requiring audit related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: agency-defined subset of AU-2a requirements (e.g. Systems capable of required event types relevant to the use or administration of FTI);

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging annually or when there is a system change. Document changes in the SSR.

AU-3: Content of Audit Records

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

Control Enhancements:

(CE-1) Additional Audit Information: Generate audit records containing the following additional information:

a. Details that facilitate the reconstruction of events if

    1. Unauthorized activity occurs or is suspected; or

    2. A malfunction occurs or is suspected.

(CE-3) Limit Personally Identifiable Information Elements: Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: agency-defined elements.

AU-4: Audit Storage Capacity

Allocate audit log storage capacity to accommodate the retention of audit records for the retention period.

AU-5: Response to Audit Processing Failures

a. Alert designated organizational officials (e.g., SA, ISSO) in the event of an audit processing failure; and

b. Take the following additional actions:

    1. Monitor system operational status using operating system or system audit logs and verify functions and performance of the system. 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

2. If logs are not available, shut down the system.

Control Enhancements:

(CE-1) Storage Warning Capacity: Provide a warning to the SA and ISSO within 24 hours when allocated audit logs storage volume reaches a specified percentage of repository maximum audit log storage capacity.

AU-6: Audit Review, Analysis and Reporting

a. Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity;

b. Report findings to the individual(s) specified within the agency's incident response procedures; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(CE-1) Automated Process Integration: Integrate audit record review, analysis, and reporting processes using automated mechanisms to support organizational processes for investigation and response to suspicious activities.

(CE-3) Correlate Audit Repositories: Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

(CE-7) Permitted Actions: Specify the permitted actions for each role or user associated with the review, analysis, and reporting of audit record information.

(CE-9) Correlation with Information from Nontechnical Sources: Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.

Supplemental Guidance: Nontechnical sources include records that document organizational policy violations related to harassment incidents and the improper use of information assets. Such information can lead to a directed analytical effort to detect potential malicious insider activity. Organizations limit access to information that is available from nontechnical sources due to its sensitive nature. Limited access minimizes the potential for inadvertent release of privacy-related information to individuals who do not have a need to know. The correlation of information from nontechnical sources with audit record information generally occurs only when individuals are suspected of being involved in an incident. Organizations obtain legal advice prior to initiating such actions.

AU-7: Audit Reduction and Report Generation

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

b. Does not alter the original content or time ordering of audit records.

Control Enhancements:

(CE-1) Automatic Processing: Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: likelihood of potential inappropriate access or unauthorized disclosure of FTI.

Supplemental Guidance: Events of interest is the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed.

AU-8: Time Stamps

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet agency-defined granularity and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

AU-9: Protection of Audit

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert ISSO upon detection of unauthorized access, modification, or deletion of audit information.

Control Enhancements:

(CE-4) Access by Subset of Privileged Users: Authorize access to management of audit logging functionality to only authorized system administrators.

AU-11: Audit Record Retention

Retain audit records **seven (7) years** to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AU-12: Audit Generation

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all systems that receive, process, store, access, protect and/or transmit FTI;

b. Allow SA and ISSO to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

Control Enhancements:

(CE-1) System-Wide and Time-Correlated Audit Trail: Compile audit records from systems that receive, process, store, access, protect and/or transmit FTI into a system-wide logical audit trail that is time-correlated to within agency-defined level of tolerance for the relationship between time stamps of individual records in the audit trail.

AU-16: Cross-Organizational Auditing Logging

Employ agency-defined methods for coordinating agency-defined audit information among external organizations when audit information is transmitted across organizational boundaries.

Supplemental Guidance: This requirement applies to consolidated and outsourced data centers, third-party vendors, and/or cloud providers handling FTI. When agencies use systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested specific services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance and privacy ramifications. Therefore, it is often the case that cross-organizational auditing simply captures the identity of individuals issuing requests at the initial system, and subsequent systems record that the requests emanated from authorized individuals.

Control Enhancements:

(CE-1) Identity Preservation: Preserve the identity of individuals in cross-organizational audit trails.

(CE-2) Sharing of Audit Information: Provide cross-organizational audit information to agency-defined organizations based on agency-defined cross-organizational sharing agreements.

4.4 ASSESSMENT, AUTHORIZATION AND MONITORING

CA-1: Assessment, Authorization and Monitoring Policy and Procedures

a. Develop, document, and disseminate to **designated agency personnel**

    1. A security and privacy assessment, authorization, and monitoring policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the security and privacy assessment, authorization and monitoring policy and the associated security and privacy assessment, authorization, and monitoring controls;

b. Designate an **agency official** to manage the security and privacy assessment, authorization and monitoring policy and procedures;

c. Review and update the current security and privacy assessment, authorization, and monitoring:

    1. Policy **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

CA-2: Control Assessments

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a control assessment plan that describes the scope of the assessment including:

    1. Controls and control enhancements under assessment;

    2. Assessment procedures to be used to determine control effectiveness; and

    3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation annually 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 and privacy requirements;

e. Produce a control assessment report that document the results of the assessment; and

f. Provide the results of the control assessment to agency's Authorizing Official (AO) or the Authorizing Official Designated Representative.

Control Enhancements:

(CE-1) Independent Assessors: Employ independent assessors or assessment teams to conduct control assessments.

Supplemental Guidance: Independent assessors or assessment teams are individuals or groups conducting impartial assessments of systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors should not create a mutual or conflicting interest with the agencies where the assessments are being conducted; assess their own work; act as management or employees of the agencies they are serving; or place themselves in positions of advocacy for the agencies acquiring their services. Independent assessments can be obtained from elements within agencies (e.g., internal audit departments, security offices, etc.) or can be contracted to public or private sector entities outside of the agency.

CA-3: Information Exchange

a. Approve and manage the exchange of information between the system and other systems using Interconnection Security Agreements (ISAs).

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the system interconnection on an annual basis.

Supplemental Guidance: This control applies to dedicated connections between two or more separate systems and does not apply to transitory, user-controlled connections such as email and website browsing. Interconnected systems falling under the same FTI environment, or authorization boundary, do not require a formal Interconnection Security Agreement.

CA-5: Plan of Action and Milestones

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the agency to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones on a quarterly basis, at a minimum, based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Supplemental Guidance: 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, access, protect and/or transmit FTI.

Control Enhancements:

(IRS-Defined): Agencies must ensure that the individual and/or office responsible for correcting each weakness is identified in the appropriate POA&M.

(IRS-Defined): Agencies must enter all new weaknesses into appropriate POA&Ms within two (2) months for weaknesses identified during assessments.

Supplemental Guidance: The results of scans/automated testing can be added to POA&Ms as multiple items or one finding per weakness for like systems.

Additional information is available in Section 2.D.9, Plan of Action and Milestones.

CA-6: Authorization

a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

    1. Accepts the use of common controls inherited by the system; and

    2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

e. Update the authorizations whenever there is a significant change to the system, or every three (3) years, whichever occurs first.

Supplemental Guidance: Authorizations are official management decisions by senior officials to authorize operation of systems and to explicitly accept the risk to agency operations and assets, individuals and other agencies based on the implementation of agreed-upon security and privacy controls. Authorizing officials provide budgetary oversight for agency systems or assume responsibility for the mission and business operations supported by those systems. Authorizing officials are responsible and accountable for security and privacy risks associated with the operation and use of agency systems. The authorization comes in the form of a memorandum signed by an agency official with fiduciary control over the security control implementation within the system. Agencies may choose to perform authorizations at the agency level (i.e., authorize all systems that receive, process, store, access, protect and/or transmit FTI at once) or at the system level (i.e., create a memo for each application and supporting infrastructure that receives, processes, stores, accesses, protects and/or transmits FTI). Authorization memos should come after processes where security controls are selected and assessed and should incorporate robust risk management processes to identify, mitigate and reduce risk to an acceptable level. Agencies may conduct ongoing authorizations of systems by implementing continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes.

CA-7: Continuous Monitoring

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establish agency-defined metrics to be monitored;

b. Establish agency-defined frequencies (no less than annually) for monitoring and agency-defined frequencies (no less than annually) for ongoing assessment of security and privacy control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to agency-defined personnel annually, at a minimum.

Control Enhancements:

(CE-1) Independent Assessors: Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

Supplemental Guidance: Agencies can maximize the value of control assessments during the continuous monitoring process by requiring that assessments be conducted by assessors with appropriate levels of independence. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not create a mutual or conflicting interest with the agencies where the assessments are being conducted; assess their own work; act as management or employees of the agencies they are serving; or place themselves in advocacy positions for the agencies acquiring their services. Independent assessments can be obtained from elements within agencies (e.g., internal audit departments, security offices, etc.) or can be contracted to public or private sector entities outside of the agency.

(CE-4) Risk Monitoring: Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

a. Effectiveness monitoring;

b. Compliance monitoring; and

c. Change monitoring.

CA-8: Penetration Testing

Conduct penetration testing every 3 years on the FTI environment.

Supplemental Guidance: Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. All parties agree to the rules of engagement before commencing penetration testing scenarios. Organizations correlate the rules of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries. Penetration testing could result in the exposure of FTI to individuals conducting the testing. Rules of engagement, contracts, or other appropriate mechanisms must be used to communicate expectations for protecting FTI. Risk assessments guide the decisions on the level of independence required for the personnel conducting penetration testing.

CA-9: Internal System Connections

a. Authorize internal connections of information system components or classes of components to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

c. Terminate internal system connections after agency-defined conditions; and

d. Review annually the continued need for each internal connection.

Control Enhancements:

(CE-1) Compliance Checks: Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.

4.5 CONFIGURATION MANAGEMENT

CM-1: Configuration Management Policy and Procedures

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

    1. An agency or organization-level configuration management policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

c. Review and update the current configuration management:

    1. Policy **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

CM-2: Baseline Configuration

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:

    1. **At a minimum annually**;

    2. When required due to **reorganizations, refreshes, etc.**; and

    3. When system components are installed or upgraded.

Control Enhancements:

(CE-2) Automation Support for Accuracy and Currency: Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms.

Supplemental Guidance: Automated mechanisms that help agencies maintain consistent baseline configurations for systems include, for example, hardware and software inventory tools, configuration management tools and network management tools. Such tools can be deployed and/or allocated at the system level, or at the operating system or component level including, for example, on workstations, servers, notebook computers, network components or mobile devices. Tools can be used, for example, to track version numbers on operating systems, applications, types of software installed and current patch levels.

(CE-3) Retention of Previous Configurations: Retain older versions of baseline configurations of the system to support rollback.

(IRS-Defined): Agencies must use SCSEMs provided on the Office of Safeguards website to ensure secure configurations of all agency information technology and communication systems receiving, processing, storing, accessing, protecting and/or transmitting FTI.

(CE-7) Configure Systems and Components for High-Risk Areas:

a. Issue a specifically configured computing device with more stringent configuration settings and the minimum-needed access to FTI to individuals traveling to locations that are deemed to be of significant risk; and

b. Apply the following controls to the systems or components when the individuals return from travel: examine for signs of tampering, reformat storage media before reintroduction to the FTI. environment

Supplemental Guidance: When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel that may include international stops or layovers. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, minimum sensitive data (e.g., FTI), and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the MP (Media Protection) family.

CM-3: Configuration Change Control

a. Determine and document the types of changes to the system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

c. Document configuration change decisions associated with the system;

d. Implement approved configuration-controlled changes to the system;

e. Retain records of configuration-controlled changes to the system for **3 years;**

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through a **Configuration Control Board** that convenes on a **monthly basis** when changes are proposed.

Control Enhancements:

(CE-2) Testing, Validation and Documentation of Changes: Test, validate, and document changes to the system before finalizing the implementation of the changes.

(CE-4) Security and Privacy Representative: Require ISSO/ISSM and Privacy Representatives to be members of the Configuration Control Board.

Supplemental Guidance: Information security representatives can include, for example, Senior Agency Information Security Officers, system security officers or system security managers. Representation by

personnel with information security expertise is important because changes to system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of organizational systems.

CM-4: Security and Privacy Impact Analyses

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Supplemental Guidance: Agency or data center personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the associated security or privacy ramifications. Security and privacy impact analyses include, for example, reviewing security and privacy plans, policies and procedures to understand security and privacy control requirements; reviewing system design documentation to understand control implementation and how specific changes might affect the controls; and determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. Impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security or privacy controls are required.

Control Enhancements:

(CE-2) Verification of Controls: After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

CM-5: Access Restrictions for Change

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Control Enhancements:

(CE-5) Privilege Limitation for Production and Operations:

a. Limit privileges to change system components and system-related information within a production or operational environment; and

b. Review and reevaluate privileges semi-annually.

(IRS-Defined): Restrict administration of configurations to only authorized administrators.

(IRS-Defined): Verify the authenticity and integrity of Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI) updates to ensure that the BIOS or UEFI is protected from modification outside of the secure update process.

Supplemental Guidance: Inventory of BIOS or UEFI information should be incorporated into existing inventory control systems, where feasible. Most agencies will rely upon the manufacturer as the source for the authenticated BIOS or UEFI. System BIOS or UEFI updates should be performed using a secure authenticated update process. After BIOS or UEFI updates, the configuration baseline should be validated to confirm that the computer system is still in compliance with the agency's defined policy. The BIOS or UEFI image and configuration baseline should be continuously monitored and deviations from the baseline should be investigated, documented, and remediated as part of incident response activities.

CM-6: Configuration Settings

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using Office of Safeguards–approved compliance tools (e.g., SCSEMs, automated assessment tools);

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 based on explicit operational requirements; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance: The authoritative source for many SCSEMs used by the Office of Safeguards is the Center for Internet Security (CIS). Office of Safeguards SCSEMs may include compliance requirements from one or more of the following additional sources:

- National Institute of Standards and Technology Special Publication 800 Series
- Internal Revenue Manuals
- Department of the Treasury guidance
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG)

(IRS-Defined): The agency shall ensure that all devices across the enterprise that store agency data are appropriately reviewed for security purposes prior to connection or reconnection to the agency's network, (e.g. checks for malicious code, updates to malware detection software, critical software updates and patches, operating system integrity and disabled hardware).

CM-7: Least Functionality

a. Configure the system to provide only mission essential capabilities and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services:

    1. Those not needed to conduct business;

    2. Those defined in the IRS Office of Safeguards approved compliance requirements (e.g., SCSEMs, assessment tools);

    3. Maintenance ports when not in use; and

    4. File Transfer Protocol (FTP).

Control Enhancements:

(CE-1) Periodic Review:

a. Review the system annually to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

b. Disable or remove identified functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure.

(CE-5) Authorized Software – Allow By Exception

a. Identify software programs authorized to execute on the system;

b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

c. Review and update the list of authorized software programs at a minimum annually.

(IRS-Defined): Periodically scan FTI networks to detect and remove any unauthorized or unlicensed software.

(CE-9) Prohibiting the Use of Unauthorized Hardware:

a. Identify agency-defined hardware components authorized for system use;

b. Prohibit the use or connection of unauthorized hardware components;

c. Review and update the list of authorized hardware components annually.

CM-8: System Component Inventory

a. Develop and document an inventory of system components that:

    1. Accurately reflects the system;

    2. Includes all components within the system;

    3. Does not include duplicate accounting of components or components assigned to any other system;

    4. Is at the level of granularity deemed necessary for tracking and reporting; and

    5. Includes the following information to achieve system component accountability: for example, hardware inventory specifications, software license information, software version numbers, component owners and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location and

b. Review and update the system component inventory at a minimum annually.

Supplemental Guidance: Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. The inventory should be sufficient to enable recovery of IT assets that are identified as lost, stolen, or disclosed.

Control Enhancements:

(CE-1) Updates During Installation and Removal: Update the inventory of system components as part of component installations, removals, and system updates.

(CE-3) Automated Unauthorized Component Detection:

a. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms at all times; and

b. Take the following actions when unauthorized components are detected:

    1. Disable network access by such components.

    2. Isolate the components.

    3. Notify designated Agency IT personnel

Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing.

CM-9: Configuration Management Plan

Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the systems development lifecycle (SDLC) and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by designated agency personnel and

e. Protects the configuration management plan from unauthorized disclosure and modification.

CM-10: Software Usage Restrictions

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; and

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.

CM-11: User-Installed Software

a. Establish policies governing the installation of software by users;

b. Enforce software installation policies through the following methods: procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both; and

c. Monitor policy compliance at a minimum annually.

CM-12: Information Location

a. Identify and document the location of FTI and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

Supplemental Guidance: This control addresses the need to understand where information is being processed and stored and is typically applied with respect to FTI. Information location includes identifying where specific information types and associated information reside in the system components that compose agency systems; and how information is being processed so that information flow can be understood, and adequate protection and policy management provided for such information and system components.

Control Enhancements:

(CE-1) Automated Tools to Support Information Location: Use automated tools to identify FTI on system components to ensure controls are in place to protect organizational information and individual privacy.

Supplemental Guidance: This control enhancement gives agencies the capability to check systems and selected system components for FTI to confirm such information resides on the component and to ensure that the required protection measures are in place for that component.

Include all FTI system and system components in the agency's FTI inventory. See NIST Control PM-29, Inventory of Personally Identifiable Information.

CM-13: Data Action Mapping

Develop and document a map of system data actions.

CM-14: Signed Components

Prevent the installation of agency-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

4.6 CONTINGENCY PLANNING

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.

CP-1: Contingency Planning Policy and Procedures

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

    1. An agency or organization-level contingency planning policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

    1. Policy **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

Supplemental Guidance: This control is applicable to all agencies receiving or storing FTI in an information technology environment. If FTI is not backed up or replicated to a secondary environment for disaster recovery purposes, the agency is required to develop and disseminate contingency planning policies prohibiting such action and supporting procedures documenting how FTI is excluded from any system backup processes. The remaining contingency planning controls would not be applicable. If FTI is backed up or replicated to a secondary environment(s) all contingency planning controls would be applicable to protect the confidentiality of FTI.

CP-2: Contingency Plan

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, assigned individuals with contact information;

    4. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;

    5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;

6. Addresses the sharing of contingency information; and

7. Is reviewed and approved by designated agency officials and other applicable agency stakeholders.

b. Distributes 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 a minimum annually;

e. Update the contingency plan to address changes to the organization, 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. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

Supplemental Guidance: Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. This control and its enhancements do not mandate a contingency plan for information systems with FTI. If agencies include their FTI information system in their contingency plan, essential mission and business functions must include ensuring the confidentiality and integrity of FTI, as well as the integrity and availability of associated records (e.g., audit logs).

Control Enhancements:

(CE-1) Coordinate with Related Plans: Coordinate contingency plan development with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for FTI include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan and Occupant Emergency Plans. Agencies should coordinate with agency IT personnel and when applicable, data center and vendor personnel to protect the confidentiality of FTI.

(CE-3) Resume Essential Missions and Business Functions: Plan for the resumption of essential mission and business functions within an agency-defined specified time-period of contingency plan activation,

(CE-8) Identify Critical Assets: Identify critical system assets supporting essential mission and business functions.

CP-3: Contingency Training

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

1. Within 30 days of assuming a contingency role or responsibility;

2. When required by system changes; and

3. Annually thereafter; and

b. Review and update contingency training content every three (3) years and following a significant change.

CP-4: Contingency Plan Testing

a. Test the contingency plan for the system at a minimum, annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: In accordance with NIST SP 800-84 Guide to Test, Training, and Exercise Process for IT Plans and Capabilities, NIST SP-34 Contingency Planning Guide for Federal Information Systems and other applicable guidance, and Business-unit Defined Tests and Exercises; and

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

Supplemental Guidance: Contingency testing templates should include: a) Name of the test, b) Name of the system(s) or environment, c) Date of the test, d) Testing point of contact, e) Purpose, type of test and scope, f) Objectives, g) Methodology, h) Activities and results (action, expected results, actual results) and i) Action item assessment.

Control Enhancements:

(CE-1) Coordinate with Related Plans: Coordinate contingency plan testing with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for FTI include, for example, business continuity plans, disaster recovery plans, continuity of operations plans, crisis communications plans, critical infrastructure plans, cyber incident response plans and occupant emergency plans. Agencies should coordinate with agency IT personnel and when applicable, data center and vendor personnel to protect the confidentiality of FTI.

CP-9: System Backup

a. Conduct backups of user-level information contained in system documentation, including security-related documentation, weekly;

b. Conduct backups of system-level information contained in the system weekly;

c. Conduct backups of system documentation, including security- and privacy-related documentation weekly; and

d. Protect the confidentiality, integrity, and availability of backup information.

Supplemental Guidance: Security-related documentation includes secure baselines, system configuration files, etc. required to maintain the secure state of systems receiving, processing, storing, accessing, protecting and/or transmitting FTI. Agencies must ensure the confidentiality and integrity of FTI if it is being backed up. This control does not mandate the backup of FTI. However, the availability and integrity of records associated with FTI (e.g., audit logs) must be ensured.

Control Enhancements:

(CE-8) Cryptographic Protection: Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of backup information containing FTI.

Supplemental Guidance: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. This control enhancement applies to system backup information in storage at primary and alternate locations to ensure only those authorized individuals have access to FTI.

CP-10: System Recovery and Reconstitution

Provide for the recovery and reconstitution of the system to a known state within agency-defined time period consistent with recovery time and recovery point objectives after a disruption, compromise, or failure.

Supplemental Guidance: Recovery is executing contingency plan activities to restore organizational missions and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point, time and reconstitution objectives and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities (including validation that the system maintains its initial security state), reestablishment of continuous monitoring activities, system reauthorizations (if required) and activities to prepare the systems against future disruptions, compromises, or failures. Recovery and reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. During system recovery and reconstitution publication 1075 requirements should be in place and functional before FTI is made accessible in the system.

Control Enhancements:

(CE-2) Transaction Recovery: Implement transaction recovery for systems that are transaction-based.

Supplemental Guidance: Transaction-based systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

4.7 IDENTIFICATION AND AUTHENTICATION

IA-1: Identification and Authentication Policy and Procedures

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

    1. An agency or organization-level identification and authentication policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current identification and authentication:

    1. Policy **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

IA-2: Identification and Authentication (Organizational Users)

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Supplemental Guidance: Organizational users include employees or individuals that agencies consider having the equivalent status of employees including, for example, contractors, data center administrators, field office users, etc. Agencies employ passwords, physical authenticators, or biometrics to authenticate user identities, or in the case of multifactor authentication, some combination thereof. Non-Organizational users are individuals or entities that interact with public-facing systems in order to complete agency transactions where FTI can be accessed (e.g., determine eligibility for benefits, review tax account, access payment histories, etc.).

Control Enhancements:

(CE-1) Multifactor Authentication to Privileged Accounts: Implement multi-factor authentication for access to privileged accounts.

Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) privileged accounts must always authenticate using multifactor options, except in the event of direct terminal access from within a restricted area (as defined in Section 2.B.3, Restricted Area Access). Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency-

controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.

(CE-2) Multifactor Authentication to Non-Privileged Accounts: Implement multi-factor authentication for access to non-privileged accounts.

Supplemental Guidance: Regardless of the type of access (i.e., local, network or remote) non-privileged accounts must always authenticate using multifactor options. Local access is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks. The use of encrypted virtual private networks for network connections between agency-controlled endpoints and non-agency-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network.

(CE-6) Access to Accounts – Separate Device: Implement multi-factor authentication for remote access to privileged accounts and non-privileged accounts such that:

a. One of the factors is provided by a device separate from the system gaining access; and

b. The device meets Authenticator Assurance Level 2 (AAL) per NIST SP 800-63.

(CE-8) Access to Accounts – Replay Resistant: Implement replay-resistant authentication mechanisms for access to privileged accounts with network access.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.

IA-3: Device Identification and Authentication

Uniquely identify and authenticate devices before establishing a remote or network connection.

Supplemental Guidance: Devices requiring unique device-to-device identification and authentication are defined by type, by device or by a combination of type and device. Organization-defined device types may include devices that are not owned by the agency. Systems use shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and wide area networks. Agencies determine the required strength of authentication mechanisms based on the security categories of systems and mission/business requirements. Because of the challenges of implementing this control on large scale, agencies can restrict the application of the control to a limited number (and type) of devices based on organizational need.

Control Enhancements:

(CE-1) Cryptographic Bidirectional Authentication: Authenticate all devices before establishing a remote network connection using bidirectional authentication that is cryptographically based.

IA-4: Identifier Management

Manage system identifiers by:

a. Receiving authorization from designated agency officials to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers indefinitely

Control Enhancements:

(CE-4) Identify User Status: Manage individual identifiers by uniquely identifying each individual as agency-defined characteristic identifying individual status (e.g., Contractor).

Supplemental Guidance: Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom agency personnel are communicating. For example, it might be useful for an agency employee to know that one of the individuals on an email message is a contractor.

(IRS-Defined): Change all default vendor-set or factory-set administrator accounts prior to implementation (e.g., during installation or immediately after installation).

IA-5: Authenticator Management

Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

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 or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators every 90 days for all user accounts and every 366 days for service accounts or when events such as loss, theft or compromise occur;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts' changes.

Control Enhancements:

(CE-1) Password-Based Authentication: For password-based authentication:

a. Maintain a list of commonly-used, expected, or compromised passwords and update the list every three (3) years and when organizational passwords are suspected to have been compromised directly or indirectly;

b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

c. Transmit passwords only over cryptographically-protected channels;

d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

e. Require immediate selection of a new password upon account recovery;

f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

g. Employ automated tools to assist the user in selecting strong password authenticators; and

h. Enforce the following composition and complexity rules:

    1. Enforce minimum password length of fourteen (14) characters.

    2. Enforce minimum password complexity to contain a combination of numbers, uppercase letters, lowercase letters, and special characters.

    3. Enforce at least one (1) character change when new passwords are selected for use.

    4. Store and transmit only cryptographically protected passwords.

    5. Enforce password lifetime restrictions:

        i. One (1) day minimum and 90 days maximum.

        ii. Service accounts passwords shall expire within 366 days (inclusive).

    6. Password History/Reuse:

        i. For all systems: 24 generations.

        ii. For systems unable to implement history/reuse restriction by generations but are able to restrict history/reuse for a specified time period, passwords shall not be reusable for a period of six (6) months.

    7. Allow the use of a temporary password for system logons with an immediate change to a permanent password.

Supplemental Guidance: If all parameters of this control are not able to be implemented through technical means, compensations and mitigations must be documented and implemented. For example: If a component is unable to enforce 4 types of characters (numbers, uppercase letters, lowercase letters, and

special characters) for complexity requirements, then the number of characters required should be increased to compensate. Users should be encouraged to make their passwords (or passphrases) as lengthy as they want, within reason.

(IRS-Defined): Train users not to use a single dictionary word as their password.

(IRS-Defined): For IT devices using a personal identification number (PIN) as an authenticator for MFA, enforce the following requirements:

a. Minimum length of eight (8) digits. If the system does not enforce a minimum length of 8 digits, the maximum length possible must be used;

b. Enforce complex sequences (e.g., 73961548 – no repeating digits and no sequential digits);

c. Do not store with the SmartCard; and

d. Do not share.

(CE-2) Public Key-Based Authentication:

a. For public key-based authentication:

    1. Enforce authorized access to the corresponding private key; and

    2. Map the authenticated identity to the account of the individual or group; and

b. When public key infrastructure (PKI) is used:

    1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and

    2. Implement a local cache of revocation data to support path discovery and validation.

(CE-5) Change Authenticators Prior to Delivery: Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.

Supplemental Guidance: This typically does not apply to developers of commercial off-the-shelf information technology products.

(CE-6) Protection of Authenticators: Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

(CE-7) No Embedded Unencrypted Static Authenticators: Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

(CE-12) Biometric Authentication Performance: For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements defined in NIST SP 800-63.

IA-6: Authenticator Feedback

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

IA-7: Cryptographic Module Authentication

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

Supplemental Guidance: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. Authentication traffic must be encrypted using the latest FIPS 140 validated cryptographic modules. A product does not meet the FIPS 140 requirements by simply implementing an approved security function. Only modules tested and validated to FIPS 140 standards meet the applicability requirements for cryptographic modules to protect sensitive information.

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

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Supplemental Guidance: Non-organizational users include system users other than organizational users explicitly covered by IA-2. Non-organizational users are individuals or entities that interact with public-facing systems in order to complete agency transactions where FTI can be accessed (e.g., determine eligibility for benefits, review tax account, access payment histories, etc.).

Control Enhancements:

(CE-2) Acceptance of External Credentials:

a. Accept only external authenticators that are NIST-compliant; and

b. Document and maintain a list of accepted external authenticators.

Supplemental Guidance: This control enhancement applies to agency systems that are accessible to the public, for example, public-facing websites or web portals. External credentials must be certified as compliant with NIST Special Publication 800-63.

(CE-4) Use of Defined Profiles: Conform to the following profiles for identity management: NIST or FICAM-issued profiles.

Supplemental Guidance: This control enhancement addresses open identity management standards. To ensure that these identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the United States Government assesses and scopes the standards and technology implementations against applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. The result is NIST-issued implementation profiles of approved protocols.

(IRS-Defined): Deploy identification and authentication technology consistent with the results of the e-authentication risk analysis.

See Section 3.3.8, Public-Facing Systems, for additional information regarding public-facing identification and authentication.

IA-9: Service Identification and Authentication

Uniquely identify and authenticate agency-defined system services and applications before establishing communications with devices, users, or other services or applications.

IA-11: Re-Authentication

Require users to re-authenticate when switching to a privileged user role.

Supplemental Guidance: In addition to the re-authentication requirements associated with device locks, agencies may require re-authentication of individuals in certain situations including, for example, when authenticators or roles change; when security categories of systems change; when the execution of privileged functions occurs; after a fixed time-period; or periodically.

IA-12: Identity Proofing

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

Supplemental Guidance: Identity proofing is the process of collecting, validating and verifying user's identity information for the purposes of issuing credentials for accessing a system. This control is intended to mitigate threats to the registration of users and the establishment of their accounts. Standards and guidelines specifying identity assurance levels for identity proofing include NIST Special Publications 800-63 and 800-63A.

Control Enhancements:

(CE-1) Supervisor Authorization: Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

(CE-2) Identity Evidence: Require evidence of individual identification be presented to the registration authority.

Supplemental Guidance: Requiring identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries. Acceptable forms of evidence are consistent with the risk to the systems, roles and privileges associated with the user's account.

(CE-3) Identity Evidence Validation and Verification: Require that the presented identity evidence be validated and verified through NIST SP 800-63 compliant methods of validation and verification.

Supplemental Guidance: Validating and verifying identity evidence increases the assurance that accounts, identifiers, and authenticators are being issued to the correct user. Validation refers to the process of confirming that the evidence is genuine and authentic, and that the data contained in the evidence is correct, current, and related to an actual person or individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying identity evidence are consistent with the risk to the systems, roles and privileges associated with the user's account.

(CE-5) Address Confirmation: Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

Supplemental Guidance: To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, agencies must use out-of-band methods to increase assurance that the individual associated with an address of record was the same person that participated in the registration.

Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts are obtained from records and not self-asserted by the user. The address can include a physical or a digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.

See Section 3.3.8, Public-Facing Systems, for additional information regarding multifactor requirements and solutions.

4.8 INCIDENT RESPONSE

Reference Section 1.8.4 Incident Response for specific instructions on incident response requirements where FTI is involved.

IR-1: Incident Response Policy and Procedures

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

    1. An agency or organization-level incident response policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the incident response policy and the associated Incident response controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

    1. Policy **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

IR-2: Incident Response Training

a. Provide incident response training to system users consistent with assigned roles and responsibilities:

    1. Within 30 days of assuming an incident response role or responsibility or acquiring system access;

    2. When required by system changes; and

    3. Annually thereafter; and

b. Review and update incident response training content every three (3) years and following major business and system change impacting the FTI environment.

Supplemental Guidance: Incident response training is linked to assigned roles and responsibilities of agency personnel to ensure the appropriate content and level of detail is included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle and remediate incidents; and finally, incident responders may receive more specific training on forensics, reporting, system recovery and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

Control Enhancements:

(CE-1) Simulated Events: Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

Supplemental Guidance: This control can be met by performing a table-top exercise using simulated events. Simulated events must include an event where FTI is compromised.

(CE-3) Breach: Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

IR-3: Incident Response Testing

Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop exercises.

Control Enhancements:

(CE-2) Coordination with Related Plans: Coordinate incident response testing with organizational elements responsible for related plans.

Supplemental Guidance: Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Occupant Emergency Plans and Critical Infrastructure Plans. Agencies should coordinate with agency IT personnel and when applicable, data center and vendor personnel to protect the confidentiality of FTI.

(CE-3) Continuous Improvement: Use qualitative and quantitative data from testing to:

a. Determine the effectiveness of incident response processes;

b. Continuously improve incident response processes; and

c. Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

IR-4: Incident Handling

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; Coordinate incident handling activities with contingency planning activities;

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, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Control Enhancements:

(CE-1) Automated Incident Handling Processes: Support the incident handling process using automated mechanisms.

Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems; and tools that support collection of live response data, full network packet capture and forensic analysis.

(CE-6) Insider Threats: Implement an incident handling capability for incidents involving insider threats.

(CE-8) Correlation with External Organizations: Coordinate with contractors, data centers, counties, and other agencies to correlate and share incidents involving FTI to achieve a cross-organization perspective on incident awareness and more effective incident responses.

Supplemental Guidance: The coordination of incident information with external organizations—including mission or business partners, customers, and developers—can provide significant benefits. Cross-organizational coordination can serve as an important risk management capability. This capability allows organizations to leverage information from a variety of sources to effectively respond to incidents and breaches that could potentially affect the organization's operations, assets, and individuals.

IR-5: Incident Monitoring

Track and document incidents.

IR-6: Incident Reporting

a. Require personnel to report suspected incidents to the organizational incident response capability immediately upon discovery; and

b. Report incident information immediately, but no later than 24 hours after identification of a possible issue involving FTI to the appropriate special agent-in-charge, TIGTA and the IRS Office of Safeguards.

Control Enhancements:

(CE-1) Automated Reporting: Report incidents using automated mechanisms.

Supplemental Guidance: Automated mechanisms for tracking incidents and for collecting and analyzing incident information include, for example, Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices.

(CE-2) Vulnerabilities Related to Incidents: Report system vulnerabilities associated with reported incidents to designated agency personnel.

Supplemental Guidance: Reported incidents that uncover system vulnerabilities are analyzed by organizational personnel including system owners, mission and business owners, senior agency information security officers, senior agency officials for privacy, authorizing officials, and the risk executive (function). The analysis can serve to prioritize and initiate mitigation actions to address the discovered system vulnerability.

(CE-3) Supply Chain Coordination: Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

Supplemental Guidance: Agencies involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving system components, information technology products, development processes or personnel and distribution

processes or warehousing facilities. Organizations determine the appropriate information to share considering the value gained from support by external organizations with the potential for harm due to controlled unclassified information being released to outside organizations of perhaps questionable trustworthiness.

IR-7: Incident Response Assistance

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or the assistance capability can proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

Control Enhancements:

(CE-1) Automation Support for Availability of Information and Support: Increase the availability of incident response information and support using automated mechanisms.

Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or the assistance capability can proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

(CE-2) Coordination with External Providers:

a. Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and

b. Identify organizational incident response team members to the external providers.

IR-8: Incident Response Plan

a. Develop an incident response plan that:

    1. Provides the organization with a roadmap for implementing its incident response capability;

    2. Describes the structure and organization of the incident response capability;

    3. Provides a high-level approach for how the incident response capability fits into the overall organization;

    4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

    5. Defines reportable incidents;

    6. Provides metrics for measuring the incident response capability within the organization;

    7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;

8. Addresses the sharing of incident information;

9. Is reviewed and approved by designated agency officials at a minimum on an annual basis; and

10. Explicitly designates responsibility for incident response to agency-defined personnel.

b. Distribute copies of the incident response plan to authorized incident response personnel and agency personnel with access to FTI;

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to authorized incident response personnel and agency personnel with access to FTI;

e. Protect the incident response plan from unauthorized disclosure and modification.

Control Enhancements:

(CE-1) Breaches: Include the following in the Incident Response Plan for breaches involving personally identifiable information:

a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;

b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and

c. Identification of applicable privacy requirements.

IR-9: Information Spillage Response

Respond to information spills by:

a. Assigning designated incident response agency personnel with responsibility for responding to information spills;

b. Identifying the specific information involved in the system contamination;

c. Alerting designated agency officials of the information spill using a method of communication not associated with the spill;

d. Isolating the contaminated system or system component;

e. Eradicating the information from the contaminated system or component;

f. Identifying other systems or system components that may have been subsequently contaminated; and

g. Performing the following additional actions: Report incident information to the appropriate special agent-in-charge, TIGTA and the IRS Office of Safeguards.

4.9 MAINTENANCE

MA-1: System Maintenance Policy and Procedures

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

    1. An agency or organization-level system maintenance policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

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

b. Designate an agency official to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current system maintenance:

    1. Policy **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

MA-2: Controlled Maintenance

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c. Require that designated agency officials explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: all information on the equipment being sanitized;

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in organizational maintenance records:

    1. Date and time of maintenance;

    2. Name of the individual performing the maintenance;

    3. Name of escort, if necessary;

    4. A description of the maintenance performed; and

5. A list of equipment removed or replaced (including identification numbers, if applicable).

MA-3: Maintenance Tools

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools **on at least an annual basis**.

Control Enhancements:

(CE-1) Inspect Tools: Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Supplemental Guidance: If, upon inspection of maintenance tools, agencies determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with agency policies and procedures for incident handling.

(CE-2) Inspect Media: Check media containing diagnostic and test programs for malicious code before the media are used in the system.

Supplemental Guidance: If, upon inspection of media containing maintenance diagnostic and test programs, agencies determine that the media contain malicious code, the incident is handled consistent with agency incident handling policies and procedures.

(CE-3) Prevent Unauthorized Removal: Prevent the removal of maintenance equipment containing organizational information by:

a. Verifying that there is no organizational information contained on the equipment;

b. Sanitizing or destroying the equipment;

c. Retaining the equipment within the facility; or

d. Obtaining an exemption from **a designated agency official(s)** explicitly authorizing removal of the equipment from the facility.

Supplemental Guidance: Organizational information includes all information specifically owned by agencies and information provided to agencies in which agencies serve as information stewards.

(CE-4) Restricted Tool Use: Restrict the use of maintenance tools to authorized personnel only.

(CE-5) Execution with Privilege: Monitor the use of maintenance tools that execute with increased privilege.

MA-4: Nonlocal Maintenance

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintain records for nonlocal maintenance and diagnostic activities; and

e. Terminate session and network connections when nonlocal maintenance is completed.

Supplemental Guidance: Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the system or system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase or biometric. Enforcing requirements in MA-4 is accomplished in part by other controls.

Control Enhancements:

(CE-1) Logging and Review:

a. Log events defined in AU-2a for nonlocal maintenance and diagnostic sessions; and

b. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

(CE-4) Authentication and Separation of Maintenance Sessions: Protect nonlocal maintenance sessions by:

a. Employing multifactor authentication consistent with NIST 800-63 Digital Identity Guidelines requirements; and

b. Separating the maintenance sessions from other network sessions with the system by either:

    1. Physically separated communications paths; or

    2. Logically separated communications paths.

(CE-6) Cryptographic Protection: Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: Virtual Private Network (VPN) connection.

(CE-7) Disconnect Verification: Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

MA-5: Maintenance Personnel

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations

Control Enhancements:

(CE-5) Non-System Maintenance: Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.

MA-6: Timely Maintenance

Obtain maintenance support and/or spare parts for security-critical information system components and/or key information technology components within the Recovery Time Objective/Recovery Point Objective (RTO/RPO) timelines and Maximum Tolerable Downtime (MTD) parameters agreed upon in the information systems Information System Contingency Plan (ISCP).

4.10 MEDIA PROTECTION

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

MP-1: Media Protection Policy and Procedures

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

    1. An agency or organization-level media protection policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:

    1. Policy **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

MP-2: Media Access

Restrict access to digital and/or non-digital media containing FTI to authorized individuals.

MP-3: Media Marking

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempt information media containing FTI from marking if the media remain within agency-controlled areas.

Supplemental Guidance: The agency must label information system media containing FTI to indicate the distribution limitations and handling caveats. This includes 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.

MP-4: Media Storage

a. Physically control and securely store digital and non-digital media containing FTI within agency-controlled areas; and

b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Reference Section 2.B, Secure Storage - IRC § 6103(p)(4)(B), on additional secure storage requirements.

MP-5: Media Transport

a. Protect and control digital and/or non-digital media containing FTI during transport outside of controlled areas using organization defined safeguards in accordance with (i) secure storage section and (ii) SC-28 control requirements;

b. Maintain accountability for system media during transport outside of controlled areas;

c. Document activities associated with the transport of system media; and

d. Restrict the activities associated with the transport of system media to authorized personnel.

Control Enhancements:

(CE-3) Custodians: Employ an identified custodian during transport of system media outside of controlled areas.

MP-6: Media Sanitization

a. Sanitize digital and non-digital media containing FTI prior to disposal, release out of organizational control, or release for reuse using NIST 800-88, Guidelines for Media Sanitization approved sanitization techniques and procedures; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Supplemental Guidance: This control applies to all system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include: digital media found in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal.

Control Enhancements:

(CE-1) Review, Approve, Track, Document, and Verify: Review, approve, track, document, and verify media sanitization and disposal actions.

(IRS-Defined): Clear or purge any sensitive data from the system BIOS or UEFI before a computer system is disposed of and leaves the agency. Reset the BIOS or UEFI to the manufacturer's default profile, to ensure the removal of sensitive settings such as passwords or keys.

(IRS-Defined): Media provided by foreign visitors (end users) may only be loaded into a standalone agency system. The system must remain standalone until such time as it is sanitized. Additionally, no other media loaded into the standalone system can be loaded into a non-standalone agency system until sanitized.

Supplemental Guidance: The control above permits, for example, foreign visitors to provide files for presentation at an agency conference or meeting provided the computer is standalone. If such a file is required for other purposes, the preferred means for obtaining it would be to ask the visitor to email it. The control also seeks to minimize the risk that malicious code on the standalone machine will be moved via media to other systems.

Additional requirements for protecting FTI during media sanitization are provided on the Office of Safeguards website.

MP-7: Media Use

a. Prohibit the use of personally-owned media on agency systems or system components; and

b. Prohibit the use of portable storage devices in agency systems when such devices have no identifiable owner.

Control Enhancements:

(IRS-Defined): Develop policy to disable all portable storage devices with the exception of those required for explicit business need, which shall be restricted to specific workstations or laptops. In the absence of an agency-developed and issued policy, the default policy is:

a. That the connection of non-agency portable storage devices is disallowed; and

b. Technical controls are implemented to enforce the policy (e.g., Implement data loss prevention software to limit the use of removable media to known devices, blacklist usb-storage, prevent the mounting of USB storage, Deny All Access to All Removable Storage Classes).

4.11 PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-1: Physical and Environmental Policy and Procedures

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

    1. An agency or organization-level physical and environmental protection policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:

    1. Policy **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

Control Enhancements:

(IRS-Defined): Develop policy and procedures as needed to address their specific building access systems (e.g., restriction of physical access, identification and authentication and audit logging), that are critical to the security of a facility.

(IRS-Defined): Develop and implement a clean desk policy for the protection of FTI (e.g., paper output, electronic storage media) to preclude unauthorized disclosures.

(IRS-Defined): Designate restricted IT areas that house IT assets such as, but not limited to, mainframes, servers, controlled interface equipment, associated peripherals and communications equipment.

PE-2: Physical Access Authorizations

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals **at least annually**; and

d. Remove individuals from the facility access list when access is no longer required.

PE-3: Physical Access Control

a. Enforce physical access authorizations at entry/exit points to facilities where the information systems that receive, process, store, access, or transmit FTI by:

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress and egress to the facility using organization-defined physical access control systems or devices.

b. Maintain physical access audit logs for organization-defined entry or exit points;

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: organization-defined physical access controls.

d. Escort visitors and control visitor activity in accordance with agency policies (e.g., personnel and physical security);

e. Secure keys, combinations, and other physical access devices;

f. Inventory organization-defined physical access devices every twelve (12) months; and

g. Change combinations and keys at least annually and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

Supplemental guidance: This control applies to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Agencies determine the types of facility guards needed including, for example, professional security staff, administrative staff, or system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Physical access control systems comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with agencies safeguarding access to such devices.

Control Enhancements:

(CE-2) Facility and Systems: Perform security checks at a minimum daily at the physical perimeter of the facility or system for exfiltration of information or removal of system components.

PE-4: Access Control for Transmission

Control physical access to information system distribution and transmission lines within agency facilities using physical security safeguards.

Supplemental Guidance: Security safeguards applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such safeguards may also be necessary to help prevent eavesdropping or modification of unencrypted transmissions. Safeguards used to control physical access to system distribution and transmission lines include, for example, locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.

PE-5: Access Control for Output Devices

Control physical access to output from output devices (e.g., monitors, printers, and audio devices) to prevent unauthorized individuals from obtaining the output.

Supplemental Guidance: Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only; placing output devices in locations that can be monitored by organizational personnel; installing monitor or screen filters; and using headphones. Output devices include, for example, monitors, printers, copiers, scanners, facsimile machines, and audio devices.

PE-6: Monitoring Physical Access

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs at a minimum **monthly** and upon occurrence of a potential indication of an event; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

Reference Section 2.B.3, Restricted Area Access, for additional information.

Control Enhancements:

(CE-1) Intrusion Alarms and Surveillance Equipment: Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

PE-8: Visitor Access Records

a. Maintain visitor access records to the facility where the system resides for **five (5) years**;

b. Review visitor access records at least **monthly**; and

c. Report anomalies in visitor access records to agency-defined personnel.

Reference Section 2.B.3.2, Authorized Access List for visitor access (AAL) requirements.

PE-16: Delivery and Removal

a. Authorize and control information system components that receive, store, process, transmit FTI entering and exiting the facility; and

b. Maintain records of the system components.

PE-17: Alternate Work Site

a. Determine and document the agency permitted alternate work sites allowed for use by employees;

b. Employ information system security and privacy controls at alternate work sites;

c. Assess the effectiveness of security and privacy controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of security or privacy incidents.

Supplemental Guidance: Alternate work sites include, for example, government facilities or private residences of employees. While distinct from alternative processing sites, alternate work sites can provide

readily available alternate locations during contingency operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations.

Reference Section 2.B.7, Alternate Work Site, for additional requirements.

4.12 PLANNING

PL-1: Planning Policy and Procedures

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

    1. An agency or organization-level planning policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the planning policy and the associated access controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current planning:

    1. Policies **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

PL-2: System Security and Privacy Plans

a. Develop security and privacy plans for the system that:

    1. Are consistent with the organization's enterprise architecture;

    2. Explicitly define the constituent system components;

    3. Describe the operational context of the system in terms of mission and business processes;

    4. Identify the individuals that fulfill system roles and responsibilities;

    5. Identify the information types processed, stored, and transmitted by the system;

    6. Provide the security categorization of the system, including supporting rationale;

    7. Describe any specific threats to the system that are of concern to the organization;

    8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

    9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

    10. Provide an overview of the security and privacy requirements for the system;

    11. Identify any relevant control baselines or overlays, if applicable;

12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;

13. Include risk determinations for security and privacy architecture and design decisions;

14. Include security- and privacy-related activities affecting the system that require planning and coordination with authorized agency personnel; and

15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation. Distribute copies of the security and privacy plans and communicate subsequent changes to the plans to **designated agency officials**;

b. Distribute copies of the plans and communicate subsequent changes to the plans to authorized agency personnel;

c. Review the plans at a minimum annually (or as a result of a significant change);

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

Supplemental Guidance: An approved and accurate SSR satisfies the requirements for the security and privacy plans (see Section 2.E.4, Safeguards Security Reports (SSR)). Security and privacy plans relate security and privacy requirements to a set of security and privacy controls and control enhancements. The plans describe how the security and privacy controls and control enhancements meet those security and privacy requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to agency operations and assets, individuals, other organizations, the state and the Nation if the plan is implemented as intended.

Security and privacy plans need not be single documents. The plans can be a collection of various documents including documents that already exist. Effective security and privacy plans make extensive use of references to policies, procedures and additional documents including, for example, design and implementation specifications where more detailed information can be obtained. This reduces the documentation associated with security and privacy programs and maintains the security- and privacy-related information in other established management and operational areas including, for example, enterprise architecture, system development life cycle, systems engineering and acquisition. Thus, security and privacy plans do not contain detailed contingency plan or incident response plan information, but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans.

Control Enhancements:

(IRS-Defined): Include or reference a plan for media sanitization and disposition that addresses all system media and backups in the agency's system security and privacy plans.

See Section MP-6: Media Sanitization for additional information on media sanitization.

PL-4: Rules of Behavior

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

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; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated.

Control Enhancements:

(CE-1) Social Media and Networking Restrictions: Include in the rules of behavior, restrictions on:

a. Use of social media, social networking sites, and external sites/applications;

b. Posting organizational information on public websites; and

c. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

(IRS-Defined): Unless superseded by centrally-issued cross-agency policy, establish usage restrictions and implementation guidance for using Internet-supported technologies (e.g. Instant messaging) based on the potential for these technologies to cause damage or disruption to the information system or the agency's accomplishment of its mission. Document the use of Internet-supporting technologies.

PL-8: Security and Privacy Architectures

a. Develop security and privacy architectures for the system that:

    1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

    2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;

    3. Describe how the architectures are integrated into and support the enterprise architecture; and

    4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures at a minimum annually to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

Supplemental Guidance: This control addresses actions taken by agencies in the design and development of systems. The security and privacy architectures at the system level are consistent with

and complement the organization-wide security and privacy architectures described in PM-7 that are integral to and developed as part of the enterprise architecture. The security and privacy architectures include an architectural description, the placement and allocation of security and privacy functionality (including security and privacy controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces and the protection mechanisms associated with each interface. In addition, the security and privacy architectures can include other information, for example, user roles and the access privileges assigned to each role, unique security and privacy requirements, types of information processed, stored and transmitted by the system, restoration priorities of information and system services and any other specific protection needs.

Control Enhancements:

(CE-1) Defense-In-Depth: Design the security and privacy architectures for the system using a defense-in-depth approach that:

a. Allocates system communication and other relevant controls to information systems processing, storing, and transmitting FTI; and

b. Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.

4.13 PROGRAM MANAGEMENT

PM-1: Information Security Program Plan

a. Develop and disseminate an organization-wide information security program plan that:

    1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

    2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities and compliance;

    3. Reflects the coordination among organizational entities responsible for information security; and

    4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, the state, and the Nation;

b. Review the organization-wide information security program plan every three (3) years and following significant changes; and

c. Protect the information security program plan from unauthorized disclosure and modification.

Supplemental Guidance: Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended. Security plans for individual systems and the organization-wide information security program plan, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the agency's information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Agencies have the flexibility to describe common controls in a single document or in multiple documents. For multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the Facilities Management Office may develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular system but instead, support multiple systems.

PM-2: Information Security Program Leadership Role

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

Supplemental Guidance: The senior information security officer is an organizational (e.g., state, local, agency, etc.) official. For federal agencies (as defined by applicable laws, Executive Orders, regulations, directives, policies, and standards), this official is the Senior Agency Information Security Officer. Agencies may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer. The senior accountable official for risk management leads the risk executive (function) in organization-wide risk management activities.

PM-3: Information Security and Privacy Resources

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;

b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and

c. Make available for expenditure, the planned information security and privacy resources.

Supplemental Guidance: Agencies consider establishing champions for information security and privacy efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Agencies may designate and empower an Investment Review Board or similar group to manage and provide oversight for the information security-and privacy-related aspects of the capital planning and investment control process.

PM-4: Plan of Action and Milestones Process

a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:

    1. Are developed and maintained;

    2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and

    3. Are reported in accordance with established reporting requirements.

b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Supplemental Guidance: The plan of action and milestones is a key document in the information security and privacy programs and is subject to reporting requirements established by the Office of Management and Budget. Organizations view plans of action and milestones from an enterprise-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities. Agency POA&Ms must include, as applicable, all recommendations from external audits, reviews, or evaluations (e.g. Office of Inspector General (OIG), Federal agencies, internal assessments or departmental compliance and assistance review reports). POA&M documents must include a risk-based criticality of each finding, actions to mitigate vulnerabilities and actions to correct deficiencies found in assessments.

PM-5: System Inventory

Develop and update continually an inventory of organizational systems.

Supplemental Guidance: This control is only for systems that process, store, or transmit FTI.

Control Enhancements:

(CE-1) Inventory of Personally Identifiable Information: Establish, maintain, and update continually an inventory of all systems, applications, and projects that process personally identifiable information.

PM-7: Enterprise Architecture

Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

Supplemental Guidance: The integration of security and privacy requirements and controls into the enterprise architecture ensures that security and privacy considerations are addressed early in the SDLC and are directly and explicitly related to the organization's mission and business processes. The process of security and privacy requirements integration also embeds into the enterprise architecture, the organization's security and privacy architectures consistent with the organizational risk management and information security and privacy strategies. For PM-7, the security and privacy architectures are developed at a system-of-systems level, representing all organizational systems. For PL-8, the security and privacy architectures are developed at a level representing an individual system. The system-level architectures are consistent with the security and privacy architectures defined for the organization. Security and privacy requirements and control integration are most effectively accomplished through the rigorous application of the Risk Management Framework and supporting security standards and guidelines.

Control Enhancements:

(IRS-Defined): Review and update the security enterprise architecture data based on the enterprise architecture timeframes.

PM-9: Risk Management Strategy

a. Develops a comprehensive strategy to manage:

    1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and

    2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;

b. Implement the risk management strategy consistently across the organization; and

c. Review and update the risk management strategy every three (3) years or as required, to address organizational changes.

Supplemental Guidance: An organization-wide risk management strategy includes, for example, an expression of the security, privacy and supply chain risk tolerance for the organization; acceptable risk assessment methodologies; security, privacy and supply chain risk mitigation strategies; a process for consistently evaluating security, privacy and supply chain risk across the organization with respect to the organization's risk tolerance; and approaches for monitoring risk over time. The senior accountable official for risk management (agency head or designated official) aligns information security management processes with strategic, operational, and budgetary planning processes. The use of a risk executive function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy organization-wide. The organization-wide risk management strategy can be

informed by security, privacy, and supply chain risk-related inputs from other sources, internal and external to the organization, to ensure the strategy is both broad-based and comprehensive.

PM-10: Authorization Process

a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;

b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c. Integrate the authorization processes into an organization-wide risk management program.

PM-12: Insider Threat Program

Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Supplemental Guidance: Insider threat programs include controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior official is designated by the department or agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department or agency insider threat policies and implementation plans; conduct host-based user monitoring of individual employee activities on government-owned computers; provide insider threat awareness training to employees; receive access to information from all offices within the department or agency for insider threat analysis; and conduct self-assessments of department or agency insider threat posture.

Insider threat programs can leverage the existence of incident handling teams that organizations may already have in place, such as cybersecurity incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace including, for example, ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues. These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts.

PM-14: Testing, Training and Monitoring

a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:

    1. Are developed and maintained; and

    2. Continue to be executed; and

b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Supplemental Guidance: This control ensures that organizations provide oversight for the security and privacy testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the three tiers of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security and privacy controls. Security and privacy training activities, while focused on individual

systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

PM-18: Privacy Program Plan

a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored, or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and

b. Review and update the policy and procedures every three (3) years or when there is a significant change.

Supplemental Guidance: A Privacy program plan is a formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program and the program management and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

Privacy program plans can be integrated with information security plans or can be represented independently, either in a single document or in compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Privacy program plans provide sufficient information about the program management and common controls (including specification of parameters and assignment and selection statements either explicitly or by reference) to enable control implementations that are unambiguously compliant with the intent of the plans and a determination of the risk incurred if the plans are implemented as intended.

The privacy plans for individual systems and the organization-wide privacy program plan together provide complete coverage for all privacy controls employed within the organization. Common controls are documented in an appendix to the organization's privacy program plan unless the controls are included in a separate privacy plan for a system. The organization-wide privacy program plan indicates which separate privacy plans contain descriptions of privacy controls.

Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the privacy program plan. If the privacy program plan contains multiple documents, the organization specifies in each document, the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls.

PM-19: Privacy Program Leadership Role

Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

Supplemental Guidance: The privacy officer described in this control is an organizational official. For federal agencies, as defined by applicable laws, Executive Orders, directives, regulations, policies, standards and guidelines, this official is designated as the Senior Agency Official for Privacy. Organizations may also refer to this official as the Chief Privacy Officer.

PM-21: Accounting of Disclosures

a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:

    1. Date, nature, and purpose of each disclosure; and

    2. Name and address, or other contact information of the individual or organization to which the disclosure was made;

b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and

c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

PM-29: Risk Management Program Leadership Roles

a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and

b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.

4.14 PERSONNEL SECURITY

PS-1: Personnel Security Policy and Procedures

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

    1. An agency or organization-level personnel security policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:

    1. Policies **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

PS-2: Position Risk Designation

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations when recruitment actions are taken or when position descriptions are rewritten.

Supplemental Guidance: The IRS Office of Safeguards requires risk designations only for agency personnel or authorized contractors with access to FTI or responsible for administering FTI environments.

PS-3: Personnel Screening

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with agency-defined conditions requiring rescreening but no less than once every five years.

See Section 2.C.3, Background Investigation Minimum Requirements for additional requirements.

PS-4: Personnel Termination

Upon termination of individual employment:

a. Disable system access within three (3) business days;

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of information security topics, specifically nondisclosure agreements;

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by terminated individual.

PS-5: Personnel Transfer

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate transfer or when warranted extended reassignment actions within five (5) business days of the formal transfer action;

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify designated agency personnel within five (5) business days of transfer.

PS-6: Access Agreements

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements **at a minimum annually**; and

c. Verify that individuals requiring access to organizational information and systems:

    1. Sign appropriate access agreements prior to being granted access; and

    2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or **at a minimum annually**.

Control Enhancements:

(CE-3) Post-Employment Requirements:

a. Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and

b. Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

PS-7: External Personnel Security

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify designated agency personnel of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within three (3) business days; and

e. Monitor provider compliance with personnel security requirements.

PS-8: Personnel Sanctions

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and

b. Notify designated agency personnel within 72 hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

PS-9: Position Descriptions

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

4.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

PT-1: Personally Identifiable Information Processing and Transparency Policy and Procedures

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

    1. An agency or organization-level personally identifiable information processing and transparency policy that:

        (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and

c. Review and update the current personally identifiable information processing and transparency:

    1. Policies **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

PT-2: Authority to Process Personally Identifiable Information

a. Determine and document the IRC § 6103 section that permits the receipt of personally identifiable information; and

b. Restrict the access of personally identifiable information to only that which is authorized.

4.16 RISK ASSESSMENT

RA-1: Risk Assessment Policy and Procedures

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

    1. An agency or organization-level risk assessment policy that:

        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

        b. Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

    2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

e. Designate an agency official to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

f. Review and update the current risk assessment:

    1. Policies **every three (3) years (or if there is a significant change)**; and

    2. Procedures **every three (3) years (or if there is a significant change)**.

RA-3: Risk Assessment

a. Conduct a risk assessment, including:

    1. Identifying threats to and vulnerabilities in the system;

    2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

    3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in system security plans and risk assessment plans;

d. Review risk assessment results at least **annually**;

e. Disseminate risk assessment results to agency-defined personnel (e.g., AO, System Owner, system administrator); and

f. Update the risk assessment at least **every three years** or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Control Enhancements:

(CE-1) Supply Chain Risk Assessment:

c. Assess supply chain risks associated with Federal Tax Information and

d. Update the supply chain risk assessment every three (3) years, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

Supplemental Guidance: Supply chain-related events include, for example, disruption, theft, use of defective components, insertion of counterfeits, malicious development practices, improper delivery practices and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity or availability of a system and its information and therefore, can also adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations, the state and the Nation. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

RA-5: Vulnerability Monitoring and Scanning

a. Monitor and scan for vulnerabilities in the system and hosted applications every thirty (30) days, prior to placing a new information system on the agency network, to confirm remediation actions, and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring 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; and

    3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities in accordance with an agency assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with agency-defined personnel to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Supplemental Guidance: Automated security scanning of assets (including wireless networks) for inventory, configuration, and vulnerability data, including at the application-level, must be included in monthly required vulnerability scans.

Control Enhancements:

(CE-2) Update by Vulnerabilities to be Scanned: Update the system vulnerabilities to be scanned at least every 30 days; prior to a new scan; when new vulnerabilities are identified and reported.

(CE-4) Discoverable Information: Determine information about the system that is discoverable and take appropriate corrective actions.

(CE-5) Privileged Access: Implement privileged access authorization to all information system components for selected vulnerability scanning activities.

Supplemental Guidance: In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain classified or controlled unclassified information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

(IRS-Defined): Implement a vulnerability management process for IT software systems (including wireless networks) to complement their patch management process.

RA-7: Risk Response

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

Supplemental Guidance: Agencies have a variety of options for responding to risk including mitigating the risk by implementing new controls or strengthening existing controls; accepting the risk with appropriate justification or rationale; sharing or transferring the risk; or rejecting the risk. Organizational risk tolerance influences risk response decisions and actions. Risk response is also known as risk treatment. This control addresses the need to determine an appropriate response to risk before a plan of action and milestones entry is generated. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately, so a plan of action and milestones entry is not needed. However, if the risk response is to mitigate the risk and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

RA-8: Privacy Impact Assessments

Conduct privacy impact assessments for systems, programs, or other activities before:

a. Developing or procuring information technology that processes personally identifiable information; and

b. Initiating a new collection of personally identifiable information that:

    1. Will be processed using information technology; and

    2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

Supplemental Guidance: A privacy impact assessment must be conducted specifically for new systems used to process, store, or transmit FTI.

4.17 SYSTEM AND SERVICES ACQUISITION

SA-1: System and Services Acquisition Policy and Procedures

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

1. An agency or organization-level system and services acquisition policy that:

   (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

   (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

b. Designate an agency designated official to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:

   1. Policy **every three (3) years (or if there is a significant change)**; and

   2. Procedures **every three (3) years (or if there is a significant change)**.

SA-2: Allocation of Resources

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

SA-3: System Development Life Cycle

a. Acquire, develop, and manage the system using an agency or organization-level system development life cycle that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the systems development lifecycle (SDLC);

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into SDLC activities.

Control Enhancements

(CE-2) Use of Live Data:

a. Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and

b. Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.

Supplemental Guidance: Live data is also referred to as operational data. The use of live data in preproduction environments can result in significant risk to agencies. Agencies can minimize such risk by using test or dummy data during the design, development and testing of systems, system components and system services. To use live FTI in a test or development environment, agencies must submit a notification as described in Section 2.E.6, Notification Reporting Requirements.

SA-4: Acquisition Process

Include the following requirements, descriptions, and criteria, explicitly or by reference, using organization-defined contract language in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements;

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

Control Enhancements

(CE-1) Functional Properties of Controls: Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

(CE-2) Design and Implementation Information for Controls: Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; organization-defined design and implementation information for the security controls to be employed at sufficient level of detail to permit analysis and testing of controls.

(CE-8) Continuous Monitoring Plan for Controls: Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.

(CE-9) Functions, Ports, Protocols and Services in Use: Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

(CE-12) Data Ownership:

a. Include organizational data ownership requirements in the acquisition contract; and

b. Require all data to be removed from the contractor's system and returned to the organization within 7 calendar days prior to contract termination.

Supplemental Guidance: The contactor must provide the agency with certification of destruction using NIST approved standards or certification that the data has been returned.

(IRS-Defined): Information systems that receive, process, store, access, protect and/or transmit FTI must be located, operated, and accessed within the United States. When a contract developer is used, agencies must document, through contract requirements, that all FTI systems (i.e., beyond commercial products used as components) are located within the United States and are developed physically within the United States by United States citizens or those with lawful resident status.

Supplemental Guidance: This includes any contractor systems or cloud environments where FTI is received, processed, stored, accessed, protected and/or transmitted. See Section 2.C.7, Offshore Operations, for additional information.

(IRS-Defined): In acquiring information technology, agencies must use common security configurations, when applicable, by (a) requiring vendors to configure IT with common security configurations (when available and applicable, e.g., Center for Internet Security benchmarks) prior to delivery or (b) configuring acquired IT to meet agency-tailored, secure parameters (e.g., configurations that meet Publication 1075 and applicable SCSEM requirements) after delivery but prior to deployment.

Supporting Guidance*:* In the latter case, agencies do not need to require that vendors securely configure IT for delivery.

SA-5: System Documentation

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

    1. Secure configuration, installation, and operation of the system, component, or service;

    2. Effective use and maintenance of security and privacy functions and mechanisms; and

    3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

    1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

    2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

    3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take agency-defined actions (e.g., recreates documentation that is essential to the effective implementation or operation of security controls) in response; and

d. Distribute documentation to designated agency officials.

SA-8: Security Engineering Principles

Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: agency-defined systems security and privacy engineering principles.

Supplemental Guidance: Agencies can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For legacy systems, agencies apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security and privacy engineering concepts and principles help to develop trustworthy, secure systems and system components and reduce the susceptibility of agencies to disruptions, hazards, threats and creating privacy-related problems for individuals. Examples of these concepts and principles include, developing layered protections; establishing security and privacy policies, architecture and controls as the foundation for design and development; incorporating security and privacy requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring security and privacy controls to meet agency and operational needs; performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns and compensating controls needed to mitigate risk. Agencies that apply security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components and system services; reduce risk to acceptable levels; and make informed risk management decisions. Security engineering principles can also be used to protect against certain supply chain risks including, for example, incorporating tamper-resistant hardware into a design.

SA-9: External System Services

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: the security and privacy requirements contained within this publication and applicable federal laws, Executive Orders, directives, policies, regulations, standards and established service-level agreements;

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: continuous monitoring activities (e.g., perform internal inspections, complete self-assessments using SCSEM, perform automated configuration compliance scans, etc.)

Control Enhancements

(CE-1) Risk Assessments and Organizational Approvals:

a. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and

b. Verify that the acquisition or outsourcing of dedicated information security services is approved by a designated agency official.

(CE-2) Identification of Functions, Ports, Protocols and Services: Require providers of external information system services that process, store, or transmit FTI to identify the functions, ports, protocols, and other services required for the use of such services.

(CE-3) Establish and Maintain Trust Relationship with Providers: Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: IRS Publication 1075 requirements for information systems that process, store, or transmit FTI.

(CE-5) Processing, Storage and Service Location: Restrict the location of accessing, processing, storage, transmission of FTI to The U.S. and territories based on IRS Publication 1075 requirements.

(CE-6) Organization-Controlled Cryptographic Keys: Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.

(CE-8) Processing and Storage Location – U.S. Jurisdiction: Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.

SA-10: Developer Configuration Management

Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service: design, development, implementation, and operation and disposal;

b. Document, manage, and control the integrity of changes to configuration items under configuration management;

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to the designated agency official.

Control Enhancements

(CE-1) Software and Firmware Integrity Verification: Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.

Supplemental Guidance: Verification of the integrity of software and firmware can be accomplished though confirmation of the hash value. For example, checksums from well-known and safe hash functions. MD5 is not considered a safe hash function to use.

(CE-3) Hardware Integrity Verification: Require the developer of the system, system component, or system service to enable integrity verification of hardware components.

(CE-7) Security and Privacy Representatives: Require agency designated security and privacy representatives to be included in the configuration change management and control process.

SA-11: Developer Testing and Evaluation

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

a. Develop and implement a plan for ongoing security and privacy assessments;

b. Perform system testing/evaluation at the depth of one or more of the following: security-related functional properties, security-related externally visible interfaces, high-level design, low-level design and/or implementation representation (i.e., source code and hardware schematics) at all post-design phases of the SDLC;

c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during testing and evaluation.

Control Enhancements

(CE-1) Static Code Analysis: Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

(CE-4) Manual Code Reviews: Require the developer of the system, system component, or system service to perform a manual code review of FTI-related applications using the following processes, procedures, and/or techniques: agency-defined manual review process.

(CE-5) Penetration Testing: Require the developer of the system, system component, or system service to perform penetration testing:

a. At the following level of rigor: at a minimum Whitebox testing; and

b. Under the following constraints: where FTI is processed, stored, or transmitted.

(CE-6) Attack Surface Reviews: Require the developer of the system, system component, or system service to perform attack surface reviews.

SA-15: Development Process, Standards and Tools

a. Require the developer of the system, system component, or system service to follow a documented development process that:

    1. Explicitly addresses security and privacy requirements;

    2. Identifies the standards and tools used in the development process;

    3. Documents the specific tool options and tool configurations used in the development process; and

    4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations at a minimum annually to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements IRS Publication 1075 security and privacy requirements.

Supplemental Guidance: Development tools include, for example, programming languages and computer-aided design systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the SDLC to track authorized changes and to prevent unauthorized changes.

Control Enhancements

(CE-3) Criticality Analysis: Require the developer of the system, system component, or system service to perform a criticality analysis:

a. At the following decision points in the system development life cycle: the agency-defined breadth/depth; and

b. At the following level of rigor: post-design phases of the SDLC.

Supplemental Guidance: This control enhancement provides developer input to the criticality analysis performed by agencies. Developer input is essential to such analysis because agencies may not have access to detailed design documentation for system components that are developed as commercial off-the-shelf products. Such design documentation includes, for example, functional specifications, high-level designs, low-level designs and source code and hardware schematics.

SA-22: Unsupported System Components

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components: Extended security support agreement that include security software patches and firmware updates from an external source for each unsupported component.

Supplemental Guidance: Support for system components includes, for example, software patches, firmware updates, replacement parts and maintenance contracts. Unsupported components, for example, when vendors no longer provide critical software patches or product updates, provide an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission or business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. Systems that no longer receive security patches or product updates may receive critical findings during Safeguards reviews. For more information on unsupported system components, see the Office of Safeguards website.

4.18 SYSTEM AND COMMUNICATIONS PROTECTION

SC-1: System and Communications Protection Policy and Procedures

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

   1. An agency or organization-level system and communications protection policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:

   1. Policy **every three (3) years (or if there is a significant change)**; and

   2. Procedures **every three (3) years (or if there is a significant change)**.

SC-2: Application Partitioning

Separate user functionality, including user interface services, from system management functionality.

Control Enhancements:

(CE-1) Interfaces for Non-Privileged Users: Prevent the presentation of system management functionality at interfaces to non-privileged users.

SC-4: Information in Shared System Resources

Prevent unauthorized and unintended information transfer via shared system resources.

SC-7: Boundary Protection

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

More information about network protections can be found in Section 3.3.6, Network Boundary and Infrastructure.

Control Enhancements:

(CE-3) Access Points: Limit the number of external network connections to the system.

(CE-4) External Telecommunications Services:

a. Implement a managed interface for each external telecommunication service;

b. Establish a traffic flow policy for each managed interface;

c. Protect the confidentiality and integrity of the information being transmitted across each interface;

d. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;

e. Review exceptions to the traffic flow policy at a minimum quarterly and remove exceptions that are no longer supported by an explicit mission or business need;

f. Prevent unauthorized exchange of control plane traffic with external networks;

g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

h. Filter unauthorized control plane traffic from external networks.

(*CE-5) Deny by Default – Allow by Exception*: Deny network communications traffic by default and allow network communications traffic by exception on information systems where FTI is accessed, processed, stored, or transmitted.

(CE-7) Prevent Split Tunneling for Remote Devices: Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using:

a. Individual users shall not have the ability to configure split tunneling

b. Auditing must be performed semi-annually on each workstation with split tunneling enabled. Auditing must include:

    1. Only those users authorized for split tunneling have it enabled in their user profile or policy object

    2. There is a continued need for split tunneling for the user

    3. Only the correct and authorized split tunneling configurations are present on the workstation

c. Host Checking is enabled and configured on the VPN server;

    1. Ensure the OS is supported

    2. Ensure that anti-malware is installed and up to date

    3. The most current hotfixes are applied

    4. Agency-defined additional parameters

(CE-8) Route Traffic to Authenticated Proxy Servers: Route internal communications traffic to external networks through authenticated proxy servers at managed interfaces.

Supplemental Guidance: External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. These system resources can include, for example, files, connections, web pages or services. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers can support logging of individual Transmission Control Protocol sessions and blocking specific Uniform Resource Locators, Internet Protocol addresses and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.

(CE-9) Restrict Threatening Outgoing Communications Traffic:

a. Detect and deny outgoing communications traffic posing a threat to external systems; and

b. Audit the identity of internal users associated with denied communications.

(CE-10) Prevent Exfiltration:

a. Prevent the exfiltration of information; and

b. Conduct exfiltration tests at least semi-annually.

(CE-11) Restrict Incoming Communications Traffic: Only allow incoming communications from agency-defined authorized sources to be routed to agency-defined authorized destinations.

(CE-12) Host-Based Protection: Implement firewalls and intrusion detection systems at access points and end user equipment as appropriate.

(CE-15) Networked Privileged Accesses: Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

(CE-17) Automated Enforcement of Protocol Format: Enforce adherence to protocol formats.

(CE-18) Fail Secure: Prevent systems from entering unsecure states in the event of an operations failure of a boundary protection area.

(IRS-Defined): Agencies shall implement and manage boundary protection (typically using firewalls) at trust boundaries. Each trust boundary shall be monitored and communications across each boundary shall be controlled.

Supplemental Guidance: For the purposes of this requirement, trust boundary is defined as a border between two connected zones with different trust levels.

Supplemental Guidance: This requirement is meant for border firewalls only. Internal firewalls used for network segmentation do not need to be stateful.

Supplemental Guidance: This capability should be placed inline. Wherever possible, intrusion prevention capabilities should be utilized.

(IRS-Defined): Agencies must block known malicious sites (inbound or outbound), as identified to the agency from US-CERT, MS-ISAC or other sources, at each Internet Access Point (unless explicit instructions are provided to agencies not to block specific sites). Blocking is to be accomplished within two business days following release of such sites.

Supplemental Guidance: US-CERT issues a monthly list of known malicious/suspicious sites as well as ad hoc notices as needed. MS-ISAC provides information to its member organizations about potential threat vectors as well.

Supplemental Guidance: Malicious beaconing activity can sometimes be detected by enabling log capture on network devices such as proxies, DNS servers and routers to record a log of possible communications with specific domains. Creating logs allows an administrator to see precisely which internal network hosts are originating communications to those domains. The internal IP addresses responsible for the communications should be the first places for incident response and mitigation for removal of malware.

SC-8: Transmission Confidentiality and Integrity

Protect the confidentiality and integrity of transmitted information.

Supplemental Guidance: 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).

Control Enhancements:

(CE-1) Cryptographic Protection: Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

(IRS-Defined): Agencies shall ensure appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed over video and voice telecommunication and teleconferences.

Supporting Guidance: Voice, video and multimedia communications can occur over traditional or digital telephone systems, cellular or other wireless networks or data networks. Transmitting voice, video, or multimedia communications over packet-switched networks (such as Local Area Networks) that were designed for data transfer rather than over dedicated circuit networks raises security concerns.

Supporting Guidance: Wireless communications are vulnerable to interception, denial of service and deception. Under any circumstances, use of wireless to transmit or receive information sensitive to disclosure can present significant risks. When implementing this policy, bureaus should recognize the convergence of (point-to-point) PTP devices with those described.

SC-10: Network Disconnect

Terminate the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity.

Supplemental Guidance: This control applies to internal and external networks. Terminating network connections associated with specific communications sessions include, for example, de-allocating associated TCP/IP address or port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include, for example, time-periods by type of network access or for specific network accesses.

SC-12: Cryptographic Key Establishment and Management

The agency must establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: NIST SP 800-57, Recommendation for Key Management, for key generation, distribution, storage, access, and destruction.

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define their key management requirements in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems.

SC-13: Cryptographic Protection

a. Determine the cryptographic uses; and

b. Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited.

SC-15: Collaborative Computing Devices and Applications

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: users are notified by signage of the presence of such devices; and

b. Provide an explicit indication of use to users physically present at the devices.

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

Control Enhancements:

(CE-4) Explicitly Indicate Current Participants: Provide an explicit indication of current participants in meetings that involve FTI.

Supplemental Guidance: Explicitly indicating current participants prevents unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.

SC-17: Public Key Infrastructure Certificates

a. Issue public key certificates under an agency-defined certificate authority or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

Supplemental Guidance: For all certificates, organizations manage system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses certificates with visibility external to organizational systems and certificates related to the internal operations of systems, for example, application-specific time services.

SC-18: Mobile Code

a. Define acceptable and unacceptable mobile code and mobile code technologies; and

b. Authorize, monitor, and control the use of mobile code within the system.

Supplemental Guidance: Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices including, for example, notebook computers and smart phones. Mobile code policy and procedures address the specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems.

Control Enhancements

(CE-1) Identify Unacceptable Code and Take Corrective Actions: Identify unacceptable mobile code and take corrective actions.

(CE-2) Acquisition, Development and Use: Verify that the acquisition, development, and use of mobile code to be deployed in the system meets IRS Publication 1075 requirements.

SC-20: Secure Name/Address Resolution Service (Authoritative Source)

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Supplemental Guidance: This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.

Control Enhancements

(CE-2) Data Origin and Integrity: Provide data origin and integrity protection artifacts for internal name/address resolution queries.

SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Supplemental Guidance: Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching DNS servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host/service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

SC-22: Architecture and Provisioning for Name/Address Resolution Service

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Supplemental Guidance: Systems that provide name and address resolution services include, for example, DNS servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers; one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles, for example, by address ranges and explicit lists.

SC-23: Session Authenticity

Protect the authenticity of communications sessions.

Supplemental Guidance: This control addresses communications protection at the session, versus packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks and session hijacking and the insertion of false information into sessions.

Control Enhancements:

(CE-1) Invalidate Session Identifies at Logout: Invalidate session identifiers upon user logout or other session termination.

(CE-3) Unique System-Generate Session Identifiers: Generate a unique session identifier for each session with session with agency-defined randomness requirements and recognize only session identifiers that are system-generated.

Supplemental Guidance: Generating unique session identifiers curtails the ability of adversaries to reuse previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.

(CE-5) Allowed Certificate Authorities: Only allow the use of agency-defined certificate authorities for verification of the establishment of protected sessions.

SC-28: Protection of Information at Rest

Protect the confidentiality and integrity of the following information at rest:

a. FTI

b. IT System-related information (e.g., configurations, rule sets);

Control Enhancements:

(CE-1) Cryptographic Protection: Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage.

SC-35: External Malicious Code Identification

Include system components that proactively seek to identify network-based malicious code or malicious websites.

SC-39: Process Isolation

Maintain a separate execution domain for each executing system process.

Supplemental Guidance: Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is readily available in most commercial operating systems that employ multi-state processor technologies.

SC-45: System Time Synchronization

Synchronize system clocks within and between systems and system components.

Control Enhancements:

(CE-1) Synchronization with Authoritative Time Source:

a. Compare the internal system clocks daily with an agency-defined authoritative time source; and

b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than agency-defined time period.

4.19 SYSTEM AND INFORMATION INTEGRITY

SI-1: System and Information Integrity Policy and Procedures

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

   1. An agency or organization-level system and information integrity policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:

   1. Policy **every three (3) years (or if there is a significant change)**; and

   2. Procedures **every three (3) years (or if there is a significant change)**.

SI-2: Flaw Remediation

a. Identify, report and correct 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 promptly after the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

Supplemental Guidance: Organizations identify systems affected by software flaws including potential vulnerabilities resulting from those flaws and report this information to designated organizational personnel with information security and privacy responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities and system error handling. By incorporating flaw remediation into ongoing configuration management processes, required remediation actions can be tracked and verified. Organization-defined time-periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. In some situations, organizations may determine that testing of software or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Control Enhancements

(CE-2) Automated Flaw Remediation Status: Determine if system components have applicable security-relevant software and firmware updates installed using automated mechanisms at a minimum monthly; daily for networked workstations and malicious code protection.

(CE-3) Time to Remediate Flaws and Benchmarks for Corrective Actions:

a. Measure the time between flaw identification and flaw remediation; and
b. Establish the following benchmarks for taking corrective actions: Agency defined based on criticality.

(CE-4) Automated Patch Management Tools: Employ automated patch management tools to facilitate flaw remediation to all FTI systems that includes but not limited to mainframes, workstations, applications, and network components

(CE-5) Automatic Software and Firmware Updates: Install security-relevant software and firmware updates automatically to all FTI systems.

(CE-6) Removal of Previous Versions of Software and Firmware: Remove previous versions of security relevant software and firmware components after updated versions have been installed.

(IRS-Defined): The agency shall ensure that, upon daily power up and connection to the agency's network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than once every 24 hours (excluding weekends, holidays, etc.)

SI-3: Malicious Code Protection

a. Implement signature-based and/or non-signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

    1. Perform periodic scans of the system and implement 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; and

    2. Either block or quarantine take and send alert to system administrator in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Control Enhancements

(IRS-Defined): All removable media must be scanned for malicious code upon introduction of the media into any system on the network and before users may access the media.

(IRS-Defined): Not less than daily, the agency shall check for updates to malicious code scanning tools, including anti-virus (AV) and anti-spyware software and intrusion detection tools and when updates are available, implement on all devices on which such tools reside.

SI-4: System Monitoring

a. Monitor the system to detect:

    1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives as defined in IT/Cybersecurity monitoring objectives as defined in the agency policy; and

    2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through a variety of techniques and methods

c. Invoke internal monitoring capabilities or deploy monitoring devices:

    1. Strategically within the system to collect organization-determined essential information; and

    2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide the output from system monitoring to designated agency officials at a minimum every two weeks or sooner if deemed necessary.

Supplemental Guidance: System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at system boundaries. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems, for example, by observing audit activities in real-time or by observing other system aspects such as access patterns, characteristics of access and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capability is achieved through a variety of tools and techniques, including, for example, intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software and network monitoring software. The distribution and configuration of monitoring devices can impact throughput at key internal and external boundaries and at other locations across a network due to the introduction of network throughput latency. Therefore, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include, for example, selected perimeter locations and near key servers and server farms supporting critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs and output from system monitoring serves as input to those programs. Adjustments to levels of system monitoring are based on law enforcement information, intelligence information or other credible

sources of information. The legality of system monitoring activities is based on applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

Control Enhancements

(CE-1) System-wide Intrusion Detection System: Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

(CE-2) Automated Tools and Mechanisms for Real-Time Analysis: Employ automated tools and mechanisms to support near real-time analysis of events.

Supplemental Guidance: Automated tools and mechanisms include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or Security Information and Event Management technologies that provide real-time analysis of alerts and notifications generated by organizational systems.

(CE-4) Inbound and Outbound Communications Traffic:

a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
b. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.

(CE-5) System-Generated Alerts: Alert the appropriate agency personnel when the following system generated indications of compromise or potential compromise occur: suspicious activity reported from firewalls, intrusion detection systems, malware detection systems, and other agency-defined security tools that report indications of compromise or potential compromise.

Supplemental Guidance: 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. Alerts can be automated, or they may be transmitted, for example, telephonically, by electronic mail messages or by text messaging. Organizational personnel on the alert notification list can include, for example, system administrators, mission or business owners, system owners, system security officers or privacy officers. This control enhancement focuses on the security alerts generated by the system. Alternatively, alerts generated by organizations in SI-4(12) focus on information sources external to the system such as suspicious activity reports and reports on potential insider threats.

(CE-10) Visibility of Encrypted Communications: Make provisions so that agency-defined encrypted communications traffic is visible to agency-defined system monitoring tools and mechanisms.

Supplemental Guidance: Organizations balance the need to encrypt communications traffic to protect data confidentiality with the need to maintain visibility into such traffic from a monitoring perspective. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.

(CE-11) Analyze Communications Traffic Anomalies: Analyze outbound communications traffic at the external interfaces to the system and selected agency defined interior points within the system to discover anomalies.

Supplemental Guidance: Agency defined interior points include subnetworks and subsystems. Anomalies within agency systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored

network protocols (e.g., IPv6 usage during IPv4 transition) and attempted communications with suspected malicious external addresses.

(CE-12) Automated Organization-Generated Alerts: Alert agency-defined personnel or roles using automated mechanisms when the following indications of inappropriate or unusual activities with security or privacy implications occur: agency-defined activities that trigger events.

(CE-18) Analyze Traffic and Covert Exfiltration: Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information at agency defined interior points within the system.

(CE-24) Indicators of Compromise: Discover, collect, and distribute to organization-defined personnel or roles, indicators of compromise provided by government and non-government sources.

(IRS-Defined): All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO.

Supplemental Guidance: If/when this information is captured and retained (one year) by DHS via Project Einstein (or a similar service) (for the Internet access point at hand) duplicative capturing/retention is not required.

SI-5: Security Alerts, Advisories and Directives

a. Receive system security alerts, advisories, and directives from third parties such as US-CERT, MS-ISAC, product vendors, etc. on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to appropriate personnel with security responsibilities (e.g., system administrators, ISSOs, system owners, incident response capabilities, etc.) and;

d. Implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.

Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) is an organization within the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) that generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, the state and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission or business partners, supply chain partners, external service providers and other peer or supporting organizations.

SI-7: Software, Firmware and Information Integrity

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: system kernels, drivers, firmware (e.g., BIOS, UEFI), software (e.g., OS, applications, middleware) and security attributes.

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: immediately disconnect the device from the network and notify designated agency officials.

Control Enhancements

(CE-1) Integrity Checks: Perform an integrity check of software, firmware, and information at startup; at the identification of a new threat to which the information system is susceptible; the installation of new hardware, software, or firmware; or at a minimum annually.

(CE-7) Integration of Detection and Response: Incorporate the detection of the following unauthorized changes into the organizational incident response capability:

a. Unauthorized changes to baseline configuration setting; and

b. Unauthorized elevation of system privileges.

(CE-10) Protection of Boot Firmware: Implement the following mechanisms to protect the integrity of boot firmware in system where FTI is accessed, processed, stored, and transmitted: verifying the checksum of downloaded firmware.

SI-8: Spam Protection

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with agency configuration management policy and procedures.

Control Enhancements

(CE-2) Automatic Updates: Automatically update spam protection mechanisms at a minimum quarterly.

SI-10: Information Input Validation

Check the validity of information inputs. (e.g., character set, length, numerical range, acceptable values).

SI-11: Error Handling

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to designated agency officials.

SI-12: Information Management and Retention

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

Control Enhancements

(CE-2) Minimize Personally identifiable Information in Testing, Training, and Research: Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: Submission of the DTR form for review and approval by IRS Office of Safeguards.

SI-16: Memory Protection

Implement the following controls to protect the system memory from unauthorized code execution: hardware-based or software-based data execution prevention.

Supplemental Guidance: 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 enforcement providing the greater strength of mechanism.

4.20 SUPPLY CHAIN RISK MANAGEMENT

SR-1: Supply Chain Risk Management Policy and Procedures

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

   1. An agency or organization-level supply chain risk management policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and

      (b) Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate an agency official to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:

   1. Policy **every three (3) years (or if there is a significant change)**; and

   2. Procedures **every three (3) years (or if there is a significant change)**.

SR-2: Supply Chain Risk Management Plan

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: Information systems that process, store, or transmit FTI

b. Review and update the supply chain risk management plan every three (3) years or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

Control Enhancements

(CE-1) Establish SCRM Team: Establish a supply chain risk management team consisting of agency-defined personnel to lead and support the following SCRM activities: provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems.

SR-3: Supply Chain Controls and Processes

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of systems that access, process, store, or transmit FTI in coordination with agency-defined supply chain personnel;

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: Agency-defined Supply Chain Risk Controls and controls identified in Pub 1075; and

c. Document the selected and implemented supply chain processes and controls in security and privacy plans; supply chain risk management plan; Agency System Security Plan.

Control Enhancements

(CE-2) Limitation of Harm: Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: agency-defined controls.

Supplemental Guidance: Controls that can be implemented to reduce the probability of adversaries successfully identifying and targeting the supply chain include avoiding the purchase of custom or non-standardized configurations, employing approved vendor lists with standing reputations in industry, following pre-agreed maintenance schedules and update and patch delivery mechanisms, maintaining a contingency plan in case of a supply chain event, using procurement carve-outs that provide exclusions to commitments or obligations, using diverse delivery routes, and minimizing the time between purchase decisions and delivery.

(CE-3) Sub-Tier Flow Down: Ensure that the controls included in the contracts of prime contractors are also included in the contracts of s.

SR-6: Supplier Assessments and Reviews

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide at a minimum annually.

SR-10: Inspection of Systems and Components

Inspect the following systems or system components at agency-defined frequency, upon delivery to detect tampering: hardware /software components that access, process, store, or transmit FTI.

SR-11: Component Authenticity

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to source of counterfeit component; agency-defined personnel or roles.

Control Enhancements

(CE-1) Anti-Counterfeit Training: Train agency-defined personnel or roles to detect counterfeit system components (including hardware, software, and firmware).

(CE-2) Configuration Control for Component Service and Repair: Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: hardware used to receive, access, process, store, transmit or protect FTI.

Exhibit 1 IRC §§ 6103(a) and (b)

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)(C) or (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 or section 6104(c), and

(3) no other person (or officer or employee thereof) who has or had access to returns or return information under subsection (c), subsection (e)(1)(D)(iii), paragraph (10), (13), or (14) of subsection (k), paragraph (6), (10), (12), (13)(A), (13)(B), (13)(C), (13)(D)(i), (16), (19), (20), or (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 a 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 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), (10), or (11), (l)(1), (2), (3), (5), (10), (11), (13)(A), (13)(B), (13)(C), (13)(D)(i), (14), (17), or (22), (o)(1)(A), or (o)(3), the Government Accountability Office, the Congressional Budget Office, or any agency, body, or commission described in subsection (d), (i)(1)(C), (3)(B)(i), or (7)(A)(ii), or (k)(10), (l)(6), (7), (8), (9), (12), (15), or (16), any appropriate State officer (as defined in section 6104(c)), or any other person described in subsection (k)(10), subsection (l)(10), (13)(A), (13)(B), (13)(C), (13)(D)(i), (16), (18), (19), or (20), or any entity described in subsection (l)(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 Government Accountability 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), (k)(10), or (l)(6), (7), (8), (9), or (16), any appropriate State officer (as defined in section 6104(c)), or any other person described in subsection (k)(10) or subsection (l)(10), (13)(A), (13)(B), (13)(C), (13)(D)(i), (16), (18), (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 (h)(2), (h)(5), (i)(1), (2), (3), (5) or (7), (j)(1), (2), or (5), (k)(8), (10), or (11), (l)(1), (2), (3), (5), (10), (11), (12), (13)(A), (13)(B), (13)(C), (13)(D)(i), (14), (15), (17), or (22), (o)(1)(A), or (o)(3) or any entity described in subsection (l)21, the Government Accountability 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

(II) 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, an appropriate State officer (as defined in section 6104(c)), or any other person described in subsection (k)(10) or subsection (l)(10), (13)(A), (13)(B), (13)(C), (13)(D)(i), (16), (18), (19), or (20) or any entity described in subsection (l)(21), or the Government Accountability 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, an appropriate State officer (as defined in section 6104(c)), or any other person described in subsection (k)(10) or subsection (l)(10), (13)(A), (13)(B), (13)(C), (13)(D)(i), (16), (18), (19), or (20) or any entity described in subsection (l)(21), or the Government Accountability 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), (10), (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)(10), (13)(A), (13)(B), (13)(C), (13)(D)(i), or (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)(10), (13)(A), (13)(B), (13)(C), (13)(D)(i), or (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 Code of Federal Regulations (CFR) § 301.6103(p)(7)-1 [T.D. 9445, 74 FR 6830, Feb. 11, 2009]

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 IRC §§ 7213 and 7213A – Sanctions for Unauthorized Disclosure and Access

IRC § 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)(1)(C), (3)(B)(i), or (7)(A)(ii), (k)(10), (13), or (14), (l)(6), (7), (8), (9), (10), (12), (15), (16), (19), (20), or (21) or (m)(2), (4), (5), (6), or (7) of section 6103 or under section 6104(c). 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 § 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 subsection (l)(18) or (n) of section 6103 or an officer or employee of such person,

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 (1)) willfully to inspect, except as authorized by this title, any return or return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2) or under section 6104(c).

(b) PENALTY

(1) IN GENERAL – Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1,000, 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 IRC § 7431 - Civil Damages for Unauthorized Inspection or Disclosure of Returns and Return Information

IRC § 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, plus

(3) in the case of a plaintiff which is described in section 7430(c)(4)(A)(ii), reasonable attorneys fees, except that if the defendant is the United States, reasonable attorneys fees may be awarded only if the plaintiff is the prevailing party (as determined under section 7430(c)(4)).

(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. The Secretary shall also notify such taxpayer if the Internal Revenue Service or a Federal or State agency (upon notice to the Secretary by such Federal or State agency) proposes an administrative determination as to disciplinary or adverse action against an employee arising from the employee's unauthorized inspection or disclosure of the taxpayer's return or return information. The notice described in this subsection shall include the date of the unauthorized inspection or disclosure and the rights of the taxpayer under such administrative determination.

(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).

(h) Special rule for information obtained under section 6103(k)(9)

For purposes of this section, any reference to section 6103 shall be treated as including a reference to section 3406.

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, disposal 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 sub-contractors. For additional information, see Section 2.E.6.2, Contractor or Sub-contractor 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 or their delegate'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., 2021–2024)
- 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 sub-contractor(s) will have access to FTI
- Name(s) and address(es) of all sub-contractor(s), if applicable

- Description of FTI to be disclosed to sub-contractor(s)
- Description of work to be performed by sub-contractor(s)
- Location(s) where work will be performed by sub-contractor(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 2.E.6.2, Contractor or Sub-contractor Access). 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

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

(1) All work will be performed under the supervision of the contractor.

(2) The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

(3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format 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 or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

(4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

(5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. 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 with a statement containing the date of destruction, description of material destroyed, and the destruction method.

(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements 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 FTI.

(8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and

obligated to the agency under this contract.

(12) For purposes of this contract, the term “contractor” includes any officer or employee of the contractor with access to or who uses FTI, and the term “subcontractor” includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI 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 FTI for a purpose not authorized 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.

(2) Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein 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.

(3) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 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 officer or employee understands the agency’s security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency’s security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on the agency’s security policy and procedures 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 the initial certification and the annual recertifications, the contractor and each officer or employee 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. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

Exhibit 8 Warning Banner Examples

A warning banner is required when access is provided to any information system that receives, processes, stores, accesses, protects and/or transmits FTI. The following elements, as explained in AC-8, System Use Notification, must be contained within the warning banner: (i) the system may contain 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 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

This table only addresses retention for documentation associated with safeguard requirements. FTI must be destroyed when there is no longer a need or use for it and in accordance with agency record retention schedules.

Table 9 Record Retention Schedules

Document Type	Document Elements	Retention Schedule
Formal Agreements	Agreement with IRS or other agency documenting IRC § 6103 authority to receive FTI from IRS or other agency See Section 1.1	Five (5) Years
Logs of FTI (FTI Log and FTI Bulk Transfer Log)	See Section 2.A.2	Five (5) Years
Converted Media	Requirements listed for FTI in its current form (electronic or non-electronic) See Section 2.A.3	Five (5) Years
State Auditor Disclosures	Approximate number of records, date of inspection, description of records, name of individual making inspection See Section 2.A.4	Five (5) Years
Visitor Access Logs	See Section 2.B.3.1	Five (5) Years
Disclosure Awareness Certification	Signed disclosure awareness confidentiality statement that certify completion and understanding of FTI security and privacy requirements See Section 2.D.2.1	Five (5) Years
Safeguard Security Report (SSR)	Reviewed in the Management Operational & Technical (MOT) Assessment See Section 2.E.4	Most Current SSR must be maintained

GLOSSARY AND KEY TERMS

Access: Access is defined as the time when an individual is permitted into some security point or system. Access also means the authority to access restricted records, such as FTI when authorized under 6103 and with a need-to-know.

Accountability: A process of holding users responsible for actions performed on an information system.

Adverse Action: A suspension of 15 days or more, a reduction in pay, or termination of employment.

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.

Banner: Display of an information system that 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.

Basic Input/Output System (BIOS): In this publication, refers collectively to boot firmware based on the conventional BIOS, Extensible Firmware Interface (EFI), and the Unified Extensible Firmware Interface (UEFI).

Blurring: The act of obscuring data so that it cannot be read or reconstructed.

Classified: National security information classified pursuant to Executive Order 12958.

Compromise: The disclosure of sensitive information to persons not authorized to receive such information.

Commingling: 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.

Contractor: Independent entity that agrees to furnish certain number or quantity of goods, material, equipment, personnel, and/or services that meet or exceed stated requirements or specifications, at a mutually agreed upon price and within a specified timeframe to another independent entity called contractee, principal, or project owner.

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.

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.

Disciplinary Action: An admonishment, written reprimand, or suspension of 14 days or less.

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.

Extensible Firmware Interface (EFI): See Unified Extensible Firmware Interface (UEFI).

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.

Exchange: An online marketplace in which individuals and small businesses can compare policies and buy insurance (with a government subsidy, if eligible).

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.

External Systems: External information systems, or non-agency-owned equipment, include any technology used to receive, process, store, access, protect and/or transmit FTI that is not owned and managed by 1) the agency or the agency-run mobile device management system, 2) a state's consolidated IT office, 3) one of the agency's approved contractors or sub-contractors (e.g., print vendors, collections agencies, application development contractors, network engineers at a state consolidated IT office, etc.) or 4) one of the agency's constituent counties. To ensure a third-party contractor system is not considered an external information system, the agency must include Exhibit 7 language in its contract with the service provider. Examples of external information systems include but are not limited to: 1) personally owned devices, which includes any device owned by an individual employee, rather than the agency itself; and 2) devices owned and managed by agency stakeholders that do not have proper approvals to receive, process, store, access, protect and/or transmit FTI.

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.

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.

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.

Local access: Is any access to agency systems by users or processes acting on behalf of users, where such access is obtained through direct connections without the use of networks.

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*.

Inadvertent Access: Access to FTI without authority that is non-willful and unanticipated or accidental.

Incidental Access: Access to FTI without a need-to-know that may occur in extraordinary circumstances (i.e., system failure, data incident response, disaster response).

Information: See *Data*.

Information Spillage: Instances where classified or controlled unclassified information (e.g., FTI) is inadvertently placed on systems that are not authorized to process such information. Such information spills occur when information that is initially thought to be of lower sensitivity is transmitted to a system and then subsequently determined to be of higher sensitivity.

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.

Insider Threat: The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of organizational operations and assets, individuals, other organizations, the state, and the nation. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information or through the loss or degradation of organizational resources or capabilities.

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.

Key: Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information.

Least privilege: A security principle under which users or processes are assigned the most restrictive set of privileges necessary to perform routine job responsibilities.

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.

Mobile code: Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

Mobile device: A computing device (other than a laptop) that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source.

Need-to-Know: Is established when individuals require FTI to perform their official duties and are authorized under the IRC.

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.

Network access: Is access to agency systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses).

Node: A device or object connected to a network.

Non-Agency-Owned Equipment: Any technology used to receive, process, store, access, protect and/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).

Object: Passive system-related entity including, for example, devices, files, records, tables, processes, programs, and domains, that contain or receive information. Access to an object (by a subject) implies access to the information it contains.

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.

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 (PII): For Safeguarding purposes, PII within this Publication refers to FTI. 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.

Personnel Sanction: A disciplinary or adverse action for individuals failing to comply with established information security policies and procedures.

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.

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.

Remote access: Access to agency systems (or processes acting on behalf of users) communicating through external networks such as the Internet. Remote access methods include, for example, dial-up, broadband, and wireless.

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.

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.

Subject: An individual, process or device causing information to flow among objects or change to the system state.

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).

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.

Unauthorized Access: Occurs when a person gains logical or physical access to FTI without authority under 6103 and without a need-to-know.

Unauthorized Disclosure: Occurs when a person with access to FTI discloses it to another person without authority under 6103.

Unified Extensible Firmware Interface (UEFI): A possible replacement for the conventional BIOS that is becoming widely deployed in new x86-based computer systems. The UEFI specifications were preceded by the EFI specifications.

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.

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

Publication 1075 (Rev. 11-2021) Catalog Number 46937O
Department of the Treasury **Internal Revenue Service** www.irs.gov