Alabama Medicaid Agency

Information Security Office

Medicaid Enterprise Security Policy – Full Set - Moderate

1.30.20

Revision History

Date	Version	Author/Owner	Description of Changes
1.9.19	0.1	Brad Bird	Initial instantiation of document
2.18.19	0.2	Brad Bird	Completion of initial policy wording for full policy set.
2.22.19	0.3	Brad Bird	Added additional IRS 1075 requirements
3.4.19	0.4	Brad Bird	Updated policy info through AU family
5.2.19	0.5	Brad Bird	Renamed – Medicaid Enterprise Security Policy – Full Set – Moderate
8.26.19	0.6	Brad Bird	Added IRS-specific language to SC-15
1.7.20	0.7	Brad Bird	Resolved comments, edited MP-6 policy language, overall updates
1.30.20	1.0	Brad Bird	Added CMS flaw remediation time frames to SI-2 policy. Moved publication out of draft into publication.

Contents

Introduction 4
Purpose 4
Authority & Applicability 4
Policy 5
Program Management 5
Access Control 14
Awareness and Training 26
Audit and Accountability 28
Assessment and Authorization 35
Configuration Management 40
Contingency Planning 47
Identification and Authentication 53
Incident Response 58
System Maintenance 62
Media Protection 65
Physical and Environmental 68
Planning 73
Personnel Security 77
Risk Assessment 81
System and Services Acquisitions 84
System and Communications Protection 90
System & Information Integrity 96
Conclusion 100
Management Commitment 101

Introduction

Reliable Information Technology (IT) resources, well-trained staff to manage those resources and strong controls to shield protected data from unauthorized disclosure, are critical to the daily operations of the Alabama Medicaid Agency (Medicaid). They enable the organization to provide quality care services essential to Alabama citizens in the most effective, efficient and safe way possible.

Demands on the services provided by technology are ever increasing, requiring more storage, faster processing, and a more controlled and secure operating environment. This increase in demand should align with an increase in secure and reliable technology and more knowledgeable staff. Medicaid's strategic goals are therefore dependent on its ability to protect the confidentiality, integrity, availability and privacy of protected information and Medicaid's IT resources.

Purpose

This policy establishes the formal Alabama Medicaid Agency information security policy, ensuring security and privacy requirements are integrated into the planning, budgeting, acquisition, and management of Medicaid information, information resources, supporting infrastructures, personnel, equipment and services.

Authority & Applicability

The authority for this publication comes under the signature of the Alabama Medicaid Agency Commissioner and the Medicaid Chief Information Officer, and is applicable to all information resources owned and managed by Medicaid and all its personnel.

Guidance used to compose this document includes, but is not limited to:

- **Alabama Medicaid Agency Administrative Code** (http://www.alabamaadministrativecode.state.al.us/docs/med/index.html)
- Alabama **security breach notification law** (2018 S.B. 318, Act No. 396) (http://arc-sos.state.al.us/PAC/SOSACPDF.001/A0012674.PDF)
- Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (**MARS-E**) ii. Version 2.0. (https://www.cms.gov/Regulations-and-Guidance/Regulations-and-Guidance.html)
- Guidance from the National Institute of Standards and technology (**NIST**) (https://csrc.nist.gov/publications/), such as:
    - Federal Information Processing Standards (FIPS): Security standards.
    - NIST Special Publications (SP) - Guidelines, technical specifications, recommendations and reference materials, comprising multiple sub-series:
        - SP 800 Computer security
        - SP 1800 Cybersecurity practice guides
        - SP 500 Information technology (relevant documents)
- Health Insurance Portability and Accountability Act (**HIPAA**) of 1996 (https://www.hhs.gov/hipaa/index.html)
- The Health Information Technology for Economic and Clinical Health (**HITECH**) Act (https://www.healthit.gov/topic/laws-regulation-and-policy/health-it-legislation)
- 45 CFR Part 95 Subpart F - Automated Data Processing (ADP) Equipment & Services (https://www.law.cornell.edu/cfr/text/45/part-95/subpart-F)

Policy

This policy intends to directly answer the Agency Internal Memorandum (AIM) 216 Minimum Protection Requirements using the security controls from the National Institute for Standards & Technology's Special Publication 800-53 revision 4. This policy also intends to incorporate all applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines by defining its requirements based off of the requirements specified by the following sources:

- Internal Revenue Service (IRS) Publication 1075
- Social Security Administration (SSA) Technical Systems Security Requirements (TSSR)
- Center for Medicare & Medicaid Services (CMS) Acceptable Risk Safeguards (ARS)
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule

Program Management

Security & Privacy Program Plan Requirement for PM

The Security & Privacy Program Plan supports Security and Privacy Program operations using program management best practices. Specific procedures, standards, products, repositories, and systems will be put into place that will require organizational participation. The end goal of Security and Privacy Program Management (PM) is to provide the structure that will consume, retain, distribute, and report security and privacy documentation to aid Medicaid in clearly understanding the risk provided to its mission by its information resources.

PM-1: Program Management Policy & Procedures

The agency:

a. Develops and disseminates 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 the responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the State.
b. Reviews the organization-wide information security program plan every three years;
c. Updates the information security program plan to address organizational changes and problems identified during plan implementation or control assessments; and
d. Protects the information security program plan from unauthorized disclosure and modification.

PM-1 HIPAA mapping

HIPAA: 45 C.F.R. §164.308 (a)(1)(i)

PM-2: Information Security Program Roles

The Agency:

a. Appoints a Senior Agency Information Security Officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program;
b. Appoints a Senior Accountable Official for Risk Management to align information security management processes with strategic, operational, and budgetary planning processes; and
c. Appoints a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.

PM-2 HIPAA mapping

45 C.F.R. §164.308(a)(2); 45 C.F.R. §164.530(a)

PM-3: Information Security & Privacy Resources

The agency:

a. Includes the resources needed to implement the information security and privacy programs in capital planning and investment requests and documents all exceptions to this requirement;
b. Prepares documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, Executive Orders, directives, regulations, standards; and
c. Makes available for expenditure, the planned information security and privacy resources.

PM-4: Plan of Action & Milestones Process

The agency:

a. Implements a process to ensure that plans of action and milestones for the security and privacy programs and associated organizational systems:
    1. Are developed and maintained;
    2. Document the remedial information security and privacy actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the State; and
    3. Are reported in accordance with established reporting requirements.
b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PM-4 HIPAA mapping

45 C.F.R. §164.310(d)

PM-5: System Inventory

The agency develops and maintains an inventory of organizational systems.

PM-6: Measures of Performance

The agency develops, monitors, and reports on the results of information security and privacy measures of performance.

PM-7: Enterprise Architecture

The agency develops and enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations, assets, individuals, other organizations, and the State.

PM-7 HIPAA mapping

45 C.F.R. §164.308(a)(1)(i)

PM-8: Critical Infrastructure Plan

The agency addresses information security and privacy issues in the development, documentation, and updating of critical infrastructure and key resources protection plan.

PM-9: Risk Management Strategy

The agency:

a. Develops a comprehensive strategy to manage:
    1. Security risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of organizational systems;
    2. Privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information; and
    3. Supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;
b. Implements the risk management strategy consistently across the organization; and
c. Reviews and updates the Risk Management Strategy annually or as required, to address organizational changes.

PM-9 HIPAA mapping

45 C.F.R. §164.308(a)(1)(ii); 45 C.F.R. §164.316(a)

PM-10: Authorization Process

The agency:

a. Manages the security and privacy state of organizational systems and the environments in which those systems operate through the authorization process;
b. Designates individuals to fulfill specific roles and responsibilities within the organization risk management process; and
c. Integrates the authorization process into an organization-wide risk management program.

PM-10 HIPAA mapping

45 C.F.R. §164.308(a)(2)

PM-11: Mission & Business Process Definition

The agency:

a. Defines organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the State;
b. Determines the information protection and personally identifiable information processing needs arising from the defined mission and business processes; and
c. Reviews and revises the mission and business processes regularly until achievable protection and personally identifiable information processing needs are obtained.

PM-11 HIPAA mapping

45 C.F.R. §164.306(a) and (b)

PM-12: Insider Threat Program

The agency implements an insider threat program that includes a cross-discipline insider threat incident handling team.

PM-13: Security and Privacy Workforce

The agency will establish a security and privacy workforce development and improvement program.

PM-13 HIPAA mapping

45 C.F.R. §164.308(a)(2)

PM-14: Testing, Training, & Monitoring

The agency:

a. Implements 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 in a timely manner;
b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PM-15: Contacts with Groups & Associations

The agency establishes and institutionalizes contact with selected groups and associations within the security and privacy communities:

a. To facilitate ongoing security and privacy education and training for organizational personnel;
b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and
c. To share current security and privacy-related information including threats, vulnerabilities, and incidents.

PM-16: Threat Awareness Program

The agency will implement a threat awareness program that includes cross-organization information sharing capability.

PM-16 (enhancement 1): Automated means for sharing threat intelligence

The agency utilizes automated means to maximize the effectiveness of sharing threat intelligence information.

PM-17: Protecting Agency Information on Non-Agency Systems

The agency:

a. Establishes policy and procedures to ensure that the requirements for the protection of Controlled Unclassified Information processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards;
b. Updates the policy and procedures every three years.

PM-18: Privacy Program Plan

The agency:

a. Develops and disseminates an organization-wide privacy program plan that provides an overview of the agency's privacy program, and:

1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;
2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;
3. Includes the role of the Senior Agency Official for Privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;
5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and
6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the State; and

b. Updates the plan to address changes in privacy laws & policy, organizational changes, and problems identified during plan implementation or privacy control assessments.

PM-19: Privacy Program Roles

The agency appoints 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.

PM-20: System of Records Notice

The agency:

a. Publishes System of Records notices in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information.
b. Keeps System of Records Notices current.

PM-21: Dissemination of Privacy Program Information

The agency:

a. Ensures that the public has access to information about organizational privacy activities and can communicate with its Senior Agency Official for Privacy;
b. Ensure that organizational privacy practices are publicly available through organizational websites or otherwise; and
c. Employ publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

PM-22: Accounting of Disclosures

The agency:

a. Develops and maintains an accounting of disclosures of personally identifiable information held in each system of records under its control, including:
    1. Date, nature, and purpose of each disclosure of a record; and
    2. Name and address of the person or organization to which the disclosure was made;
b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and
c. Makes the accounting of disclosures available to the person named in the record upon request.

PM-23: Data Quality Management

The agency issues guidelines ensuring and maximizing the quality, utility, objectivity, integrity, impact determination, and de-identification of personally identifiable information across the information life cycle.

PM-24: Data Management Board

The agency:

a. Will establish a written charter for a Data Management Board;
b. Will establish the Data Management Board consisting of organization-defined roles with the following responsibilities:
    1. Develop and implement guidelines supporting data modeling, quality, integrity, and de-identification needs of personally identifiable information across the information life cycle;
    2. Review and approve applications to release data outside of the organization, archiving the applications and the released data, and performing post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid;
c. Includes requirements for personnel interaction with the Data Management Board in security and privacy awareness and/or role-based training.

PM-25: Data Integrity Board

The agency will establish a Data Integrity Board to oversee organizational Computer Matching Agreements.

PM-26: Minimization of Personally Identifiable Information used in Testing, Training, and Research

The agency:

a. Develops and implements policies and procedures that address the use of personally identifiable information for internal testing, training, and research;

b. Takes measures to limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes; and
c. Authorizes the use of personally identifiable information when such information is required for internal testing, training, and research.

PM-27: Individual Access Control

The agency:

a. Publishes:
    1. Policies governing how individuals may request access to records maintained in a Privacy Act system of records; and
    2. Access procedures in System of Records Notices; and
b. Ensures that the published policies and access procedures are consistent with Privacy Act requirements and Office of Management and Budget policies and guidance for the proper processing of Privacy Act requests.

PM-28: Complaint Management

The agency implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices that includes:

a. Mechanisms that are easy to use and readily accessible by the public;
b. All information necessary for successfully filing complaints; and
c. Tracking mechanisms to ensure all complaints received are reviewed and appropriately addressed in a timely manner.

PM-29: Inventory of Personally Identifiable Information

The agency:

a. Establishes, maintains, and updates an inventory of all programs and systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information;
b. Provide updates of the personally identifiable information inventory to the Chief Information Officer, Senior Agency Official for Privacy, and Senior Agency Information Security Officer annually;
c. Uses the personally identifiable information inventory to support the establishment of information security and privacy requirements for all new or modified systems containing personally identifiable information;
d. Reviews the personally identifiable information inventory annually;
e. Ensures to the extent practicable, that personally identifiable information is accurate, relevant, timely, and complete; and
f. Reduce personally identifiable information to the minimum necessary for the proper performance of authorized organizational functions.

PM-30: Privacy Reporting

The agency develops, disseminates, and updates privacy reports to:

a. Applicable oversight bodies to demonstrate accountability with statutory and regulatory privacy program mandates; and
b. Organizational personnel with responsibility for monitoring privacy program progress and compliance.

PM-31: Supply Chain Risk Management Plan

The agency:

a. Develops a plan for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;
b. Implements the supply chain risk management plan consistently across the organization; and
c. Review and update the supply chain risk management plan every three years or as required, to address organizational changes.

PM-32: Risk Framing

The agency:

a. Identifies assumptions affecting risk assessments, risk response, and risk monitoring;
b. Identifies constraints affecting risk assessments, risk response, and risk monitoring;
c. Identify the organizational risk tolerance; and
d. Identifies priorities and trade-offs considered by the organization for managing risk.

Access Control

AIM 216 Minimum Protection Requirement for AC

The Agency will limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

The following specific controls detail how the agency intends to meet the Minimum Protection Requirement for Access Control.

AC-1: Access Control Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. An 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 the associated access controls;
b. Designates the Chief Information Security Officer to manage the access control policy and procedures;
c. Reviews and updates the current access control:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the access control procedures implement the access control policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the access control policy.

AC-1 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.514(d)(1)-(5)

AC-2: Account Management

The agency:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, application, guest/anonymous, emergency, and temporary;
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;

d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by:
    - The Agency Commissioner, Deputy Commissioners, Business Owners/Program Manager, Directors, Associate Directors or Supervisors; and
    - Human Resources; and
    - The Information Security Office
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with organizational account management policies, standards, and procedures;
g. Monitors the use of information system accounts;
h. Notifies account managers:
    - When accounts are no longer required;
    - When users are terminated or transferred; and
    - When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
    - A valid access authorization;
    - Intended system usage; and
    - Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements
    - For Moderate systems at least every 90 days
    - For Low systems at least every 365 days; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
l. Aligns account management processes with personnel termination and transfer processes.

AC-2 (enhancement 1): Automated System Account Management

The Agency employs automated mechanisms to support the management of information system accounts.

AC-2 (enhancement 2): Removal of Temporary and Emergency Accounts

Agency systems automatically disable emergency accounts within 24 hours; and temporary accounts with a fixed duration not to exceed 60 days.

AC-2 (enhancement 3): Disable Inactive Accounts

Agency systems automatically disable inactive accounts within 60 days.

AC-2 (enhancement 4): Automated Audit Actions

Agency systems automatically audit account creation, modification, enabling, disabling, and removal actions and notify the Security Operations Center and other roles and personnel as required.

AC-2 (enhancement 5): Inactivity Logout

The Agency requires that users log out when the time-period of inactivity exceeds 90 minutes and at the end of the user's normal work period.

AC-2 (enhancement 10): Shared and Group Account Credential Change

Agency systems update shared/group account credentials when members leave the group.

AC-2 (enhancement 13): Disable accounts for high-risk individuals

The Agency disables accounts of users posing a significant risk immediately, not to exceed 60 minutes after discovery of the risk.

AC-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(a)(2)(i); 45 C.F.R. §164.502

AC-3: Access Enforcement

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

AC-3 (enhancement 9): Controlled Release

The Agency releases information outside of the established system boundary only if:

a) The receiving system, system component, or entity provides the requirements as described in the "PM-17: Protecting Agency Information on non-Agency Systems" requirements; and
b) A Privacy Impact Assessment and Security Assessment (against the above stated requirements) are used to validate the appropriateness of the information designated for release.

AC-3 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(a)(2)(ii), 45 C.F.R. §164.312(a)(2)(iv)

AC-4: Information Flow Enforcement

Agency systems enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

AC-4 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.310(b)

AC-4 Additional IRS 1075 requirements

The agency does not process, transmit, or store Federal Tax Information through email communications, Fax equipment, or Multi-functional devices.

AC-5: Separation of Duties

The Agency:

a. Separates duties of individuals as necessary, enforced by role-based access control whenever possible, to prevent malicious activity without collusion;
b. Documents separation of duties of individuals; and
c. Defines information system access authorizations to support separation of duties.

AC-5 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(i), 164.308(a)(4)(i), 45 C.F.R. §164.308(a)(4)(ii)(A), 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(c)(1)

AC-6: Least Privilege

The agency employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational mission and business functions.

AC-6 (enhancement 1): AUTHORIZE ACCESS TO SECURITY FUNCTIONS

At a minimum, the agency explicitly authorizes access to the following list of security functions (deployed in hardware, software, and firmware) and security-relevant information:

a. Setting/modifying audit logs and auditing behavior;
b. Setting/modifying boundary protection system rules;
c. Configuring/modifying access authorizations (i.e., permissions, privileges);
d. Setting/modifying authentication parameters; and
e. Setting/modifying system configurations and parameters.

AC-6 (enhancement 2): NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

At a minimum, the agency requires that users of information system accounts, or roles, with access to the following list of security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions:

a. Setting/modifying audit logs and auditing behavior;
b. Setting/modifying boundary protection system rules;
c. Configuring/modifying access authorizations (i.e., permissions, privileges);
d. Setting/modifying authentication parameters; and
e. Setting/modifying system configurations and parameters.

AC-6 (enhancement 5): PRIVILEGED ACCOUNTS

The agency restricts privileged accounts on the information system to personnel or roles requiring privileged access to perform specific activities required by a specific role.

AC-6 (enhancement 7): REVIEW OF USER PRIVILEGES

The Agency:

a. Reviews the privileges assigned to personnel or roles annually to validate the need for such privileges; and
b. Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

AC-6 (enhancement 9): AUDITING USE OF PRIVILEGED FUNCTIONS

Agency systems audit the execution of privileged functions.

AC-6 (enhancement 10): PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

Agency systems prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

AC-6 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.502(b), 45 C.F.R. §164.308(a)(4)(ii)(A), 45 C.F.R. §164.312(a)(1)

AC-6 Additional IRS 1075 Requirements

The agency:

- Explicitly authorizes access to Federal Tax Information;
- Requires that users of information system accounts, or roles, with access to FTI, use non-privileged accounts or roles when accessing non-security functions;
- Restricts privileged accounts on the information system to a limited number of individuals with a need to perform administrative duties;
- Audits the execution of privileged functions; and
- Prevent non-privileged users from executing privileged functions; including disabling, circumventing, or altering implemented security safeguards/countermeasures.

AC-7: Unsuccessful Logon Attempts

Agency systems:

a. Enforce the limit of consecutive invalid login attempts by a user to 5 attempts within 120 minutes; and
b. Automatically disables or locks the account/node until released by an administrator or after 1 hour when the maximum number of unsuccessful attempts is exceeded.

AC-7 Additional IRS 1075 Requirements

With respect to agency systems the process, store, or transmit Federal Tax Information, the systems:

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

AC-8: System Use Notification

Agency Systems:

a. Display an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner states:

   Please read the following agreement carefully.

   This is a government system for AUTHORIZED OFFICIAL USE 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, USC Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Title 26, USC, Sections 7213, 7213A the Taxpayer Browsing Protection Act, and 7431 in addition to possible other federal and state of Alabama criminal and civil penalties. This system and equipment is 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.

   Reference Medicaid HIPAA Security Policy S600-06 Computer Acceptable Use, for additional information.

   ---

b. Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and
c. For publicly accessible systems:
    a. Display system use information when appropriate, before granting further access;
    b. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
    c. Include a description of the authorized uses of the system.

AC-8 HIPAA mapping

45 C.F.R. §164.520(1)(i)

AC-8 Additional IRS 1075 Requirements

Before granting access to an agency system that receives, processes, stores, transmits, or disposes of Federal Tax Information, the system (and each applicable system component – i.e. application, database, operating system, and network devices) displays to users an IRS-approved warning banner that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

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

Further, the system (and applicable system components) must Retain the warning banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

The agency does not make Federal Tax Information publicly available through its systems.

AC-11: Device Lock

Agency systems:

a. Prevent further access to the system by initiating a session lock after fifteen (15) minutes of inactivity (for both remote and internal access connections) or upon receiving a request from a user; and
b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.

AC-11 (enhancement 1): PATTERN-HIDING DISPLAYS

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

AC-11 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(b), 45 C.F.R. §164.312(a)(2)(iii), 45 C.F.R. §164.312(a)(1)

AC-12: Session Termination

Agency systems automatically terminate a user session after 30 minutes of inactivity.

AC-14: Permitted Actions without identification or authentication

The Agency:

a. Identifies specific user actions that can be performed on the information system without identification or authentication;
b. Documents and provides supporting rationale in the system security plan for the information system, user actions not requiring identification or authentication; and
c. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

AC-14 HIPAA mapping

45 C.F.R. §164.312(a)(2)(i)

AC-14 Additional IRS 1075 Requirements

Federal Tax Information may not be disclosed to individuals on the information system without identification and authentication.

AC-17: Remote Access

The agency:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorizes remote access to the system prior to allowing such connections.

AC-17 (enhancement 1): Automated monitoring and control

Agency systems monitor and control remote access methods.

AC-17 (enhancement 2): Protection of Confidentiality and Integrity using Encryption

Agency systems implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AC-17 (enhancement 3): Managed Access Control Points

Agency systems route all remote accesses through a limited number of managed network access control points.

AC-17 (enhancement 4): Privileged Commands and Access

Agency systems:

a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and
b) Documents the rationale for such access in the system security plan.

AC-17 (enhancement 9): Disconnect/Disable Access

Agency systems provide the capability to expeditiously disconnect or disable remote access to the system within one (1) hour.

AC-17 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(c); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(e)(1); 45 C.F.R. §164.312(b); 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(e)(2)(ii)

AC-17 Additional IRS 1075 Requirements

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

FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies, or military installations.

Further, FTI may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore.

AC-18: Wireless Access

The agency:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access;
b. Authorizes wireless access to the information system prior to allowing such connections.

AC-18 (enhancement 1): AUTHENTICATION AND ENCRYPTION

Agency systems protect wireless access to the system using encryption, and authentication of both users and devices.

AC-18 (enhancement 3): DISABLE WIRELESS NETWORKING

Agency systems disable, when not intended for use, wireless networking capabilities internally embedded within system components prior to issuance and deployment.

AC-18 Additional IRS 1075 Requirements

Agency systems that receive, process, store, transmit, or dispose of Federal Tax Information must employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

Detailed mandatory requirements for using FTI on an 802.11 wireless LAN can be found in section 9.4.18 of IRS Publication 1075.

AC-19: Access Control for Mobile Devices

The agency:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices;
b. CIO or his/her designee authorizes the connection of mobile devices to organizational information systems; and
c. Protects and control mobile devices when outside of controlled areas.

AC-19 (enhancement 5): FULL DEVICE AND CONTAINER-BASED ENCRYPTION

The agency employs (FIPS 140-2 validated module) full-device encryption or container encryption to protect the confidentiality and integrity of information on approved mobile devices.

AC-19 Additional IRS 1075 Requirements

Agency systems that use mobile devices (as defined by the Security Program - Glossary – excluding Laptops) to receive, process, store, transmit, or dispose of Federal Tax Information must purge/wipe information from mobile devices based on 10 consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones and tablets).

Detailed mandatory requirements for using FTI on mobile devices can be found in section 9.4.8 of IRS Publication 1075.

AC-20: Use of External Systems

The agency prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designee.

If external information systems are authorized, the agency establishes strict terms and conditions for their use. The terms and conditions must address, at a minimum:

a. The types of applications that can be accessed from external information systems;
b. The maximum RA-2 security category of information that can be processed, stored, and transmitted;
c. How other users of the external information system will be prevented from accessing agency information;
d. The use of VPN and stateful inspection firewall technologies;
e. The use of and protection against the vulnerabilities of wireless technologies;
f. The maintenance of adequate physical security controls;
g. The use of virus and spyware protection software; and
h. How often the security capabilities of installed software are to be updated.

AC-20 (enhancement 1): LIMITS ON AUTHORIZED USE

The agency permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the agency:

a. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

AC-20 (enhancement 2): PORTABLE STORAGE DEVICES

The agency restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems.

AC-20 HIPAA mapping

45 C.F.R. §164.312(a)(2)(i); 45 C.F.R. §164.314(a)

AC-20 Additional IRS 1075 Requirements

With respect to receiving, processing, storing, transmitting, or disposing of Federal Tax Information, the agency does not permit:

a. Access to FTI from external information systems, other than through a virtual desktop infrastructure;
b. The use of agency-controlled portable storage devices (e.g., flash drives, external hard drives) containing FTI on external information systems;
c. The use of non-agency-owned information systems; system components; or devices to process, store, or transmit FTI; any non-agency-owned information system usage requires the agency to notify the Office of Safeguards 45 days prior to implementation.

AC-21: Information Sharing

The agency:

a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved information-sharing circumstances where user discretion is required; and
b. Employs automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

AC-21 HIPAA mapping

45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.308(b)(1); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.314(a)

AC-21 Additional IRS 1075 Requirements

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

AC-22: Publicly Accessible Content

The agency:

a. Designates individuals authorized to post information onto a publicly accessible information system;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d. Reviews the content on the publicly accessible information system for nonpublic information bi-weekly and removes such information, if discovered.

AC-22 HIPAA mapping

45 C.F.R. §164.502(a)

AC-22 Additional IRS 1075 requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency:

a. Trains authorized individuals to ensure that publicly accessible information does not contain FTI;
b. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that FTI is not included; and
c. Reviews the content on the publicly accessible information system for FTI, at a minimum, quarterly and removes such information, if discovered.

Awareness and Training

AIM 216 Minimum Protection Requirement for AT

The Agency will: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

AT-1: Awareness & Training Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. An Awareness & 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 & Training policy and the associated security and privacy awareness & training controls;
b. Designates the Chief Information Security Officer to manage the Awareness & Training policy and procedures;
c. Reviews and updates the current Awareness & Training:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the Awareness & Training procedures implement the Awareness & Training policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the Awareness & Training policy.

AT-1 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(5)(i), 45 C.F.R. §164.308(a)(5)(ii)(A), 45 C.F.R. §164.308(a)(5)(ii)(B)

AT-2: Awareness Training

The agency provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users prior to accessing any system's information;
b. When required by system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

AT-2 (enhancement 2): INSIDER THREAT

The agency includes security awareness and training on recognizing and reporting potential indicators of insider threats, such as:

a. Inordinate, long-term job dissatisfaction,
b. Attempts to gain access to information not required for job performance,
c. Unexplained access to financial resources,
d. Bullying or sexual harassment of fellow employees,
e. Workplace violence, and
f. Other serious violations of organizational policies, procedures, directives, rules, or practices.

AT-2 HIPAA mapping

HIPAA: 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 45 C.F.R. §164.308(a)(5)(ii)

AT-2 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, Section 6.3 Disclosure Awareness Training in IRS Publication 1075 is required in order for authorized individuals to gain access to Federal Tax Information.

AT-3: Role-Based Training

The agency provides role-based security training to personnel (both contractor and employee) with assigned information security and privacy roles and responsibilities (i.e., significant information security and privacy responsibilities):

a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. Within sixty (60) days of entering a position that requires role-specific training, and within every 365 days thereafter.

AT-4: Training Records

The agency:

a. Identifies employees and contractors who hold roles with significant information security and privacy responsibilities;
b. Documents and monitors individual information system security and privacy training activities, including basic security and privacy awareness and training and specific role-based information system security and privacy training; and
c. Retains individual training records for a minimum of five (5) years after the individual completes each training.

AT-4 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(5)(i); 45 C.F.R. §164.308(a)(5)(i); 45 C.F.R. §164.530(b)(2)(ii)

Audit and Accountability

AIM 216 Minimum Protection Requirement for AU

The Agency will: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

AU-1: Audit & Accountability Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. An Audit & 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 & Accountability policy and the associated Audit & Accountability controls;
b. Designates the Chief Information Security Officer to manage the Audit & Accountability policy and procedures;
c. Reviews and updates the current Audit & Accountability:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the Audit & Accountability procedures implement the Audit & Accountability policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the Audit & Accountability policy.

AU-1 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D)

AU-2: Audit Events

The agency:

a. Determines that the information system can audit the following events:
    - Server alerts and error messages;
    - User log-on and log-off (successful or unsuccessful);
    - All system administration/privileged account activities;
    - Account switching or running privileged account from non-privileged accounts (e.g. linux/unix SU or Windows RUNAS);
    - Modification of privileges and access;
    - Creation or Modification of privileged user groups;

- Privileged-level commands that can performed in a user role;
- Start up and shut down;
- Application modifications;
- Application or database modifications by batch file or process;
- Application-critical record changes;
- Application alerts and error messages;
- Changes to database or application records, where the application has been bypassed to produce the change (e.g., via file or database utility);
- All system and data interactions concerning Federal Tax Information;
- Configuration changes;
- Account creation, modification, or deletion;
- Password change;
- File creation and deletion;
- Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su)
- Read access to sensitive information;
- Modification to sensitive information;
- Printing sensitive information;
- Anomalous (e.g., non-attributable) activity;
- Data as required for privacy monitoring privacy controls;
- Concurrent log on from different work stations;
- Override of access control mechanisms; and
- Process creation;
- Audit log clearing;
- Start/Stop of audit functions;
- Remote access outside of the corporate network communication channels (e.g., IPSec or SSL VPN);

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the auditable events are deemed to be adequate (relevant) to support after-the-fact investigations of security and privacy incidents; and
d. Determines which events specified in the AU Audit and Accountability Standards require auditing on a continuous basis in response to specific situations.

AU-2 (enhancement 3): Reviews and Updates

The agency reviews and updates the list of auditable events no less often than every three hundred sixty-five (365) days and whenever there is a significant system modification.

AU-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(C), 45 C.F.R. §164.312(b), 45 C.F.R. §164.308(a)(1)(ii)(D)

AU-2 Additional IRS 1075 Requirements

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

by each unique user. With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, agency systems must meet the auditing requirements in IRS Publication 1075 section 9.3.3.2 Audit Events.

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

AU-3: Content of Audit Records

Agency systems generate audit records containing information that specifies:

- Date and time of the event;
- Component of the information system (e.g., software component, hardware component) where the event occurred;
- Type of event;
- User/subject identity;
- Outcome (success or failure) of the event;
- Execution of privileged functions; and
- Command line (for process creation events).

AU-3 (enhancement 1): Additional Audit Information

Agency systems generate audit records containing the following additional, more detailed information:

- Filename accessed;
- Program or command used to initiate the event; and
- Source and destination addresses.

AU-3 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C)

AU-3 Additional IRS 1075 Requirements

Generate audit records containing details to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected in the audit records for audit events identified by type, location, or subject.

AU-4: Audit Storage Capacity

The agency allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

AU-4 HIPAA mapping

HIPAA: 164.312(b);

AU-4 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency must allocate audit record storage capacity to retain audit records for the required audit retention period of seven years.

AU-5: Response to Audit Processing Failures

Agency systems:

a. Alerts the Security Operations Center and Systems Administrators in the event of an audit processing failure; and
b. Takes the following actions in response to an audit failure or audit storage capacity issue:
    - For Low categorized systems and systems hosting information not deemed sensitive – remediate audit failures as support resources are available;
    - For Moderate categorized systems and systems hosting information deemed sensitive – remediate audit failures within 5 days, increase storage capacity when needed within 1 day.

AU-5 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the auditing capability must:

- provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity; and
- Monitor system operational status using operating system or system audit logs and verify functions and performance of the system.

Logs shall be able to identify where system process failures have taken place and provide information relative to corrective actions to be taken by the system administrator.

AU-6: Audit, Review, Analysis, & Reporting

The agency:

a. Reviews and analyzes system audit records at least weekly or more frequently for indications of inappropriate or unusual activity, or policy non-compliance; and
b. Reports findings to the Chief Information Security Officer, Information Security Office/Security Operations Center, Systems Administrators and other applicable roles as necessary; and
c. Adjusts the level of audit 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.

AU-6 (enhancement 1): Automated Process Integration

The agency employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

AU-6 (enhancement 3): Correlate Audit Responses

The agency analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

AU-6 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(5)(ii)(C), 45 C.F.R. §164.312(b)

AU-6 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency reports findings according to the agency incident response policy. If the finding involves a potential unauthorized disclosure of FTI, the appropriate special agent-in-charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards must be contacted, as described in Section 10.0, Reporting Improper Inspections or Disclosures of IRS Publication 1075.

AU-7: Audit Reduction & Report Generation

Agency systems provide an audit reduction and report generation capability that:

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

AU-7 (enhancement 1): Automatic Processing

Agency systems provide the capability to process audit records for events of interest based on selectable event criteria.

AU-7 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.312(b)

AU-8: Time Stamps

Agency systems:

a. Use internal system clocks to generate time stamps for audit records; and
b. Record time stamps for audit records that can be mapped to UTC or Greenwich Mean Time (GMT) and is accurate to within one hundred (100) milliseconds.

AU-8 (enhancement 1): Synchronization with Authoritative Time Source

The information system:

a. Compares the internal information system clocks no less often than daily and at system boot with one or more of the following state or federally maintained NTP stratum-1 servers:
    - NIST Internet Time Servers (http://tf.nist.gov/tf-cgi/servers.cgi)
    - State or Agency designated internal NTP time servers; and

b. Synchronizes the internal clocks to the authoritative time source when the time difference is greater than one hundred (100) milliseconds

AU-9: Protection of Audit Information

Agency systems protect audit information and audit tools from unauthorized access, modification, and deletion.

AU-9 (enhancement 4): Access by subset of privileged users

The organization authorizes access to management of audit functionality to only those individuals or roles who are not subject to audit by that system. System and network administrators must not have the ability to modify or delete audit log entries.

AU-9 HIPAA mapping

45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b)

AU-11: Audit Record Retention

The agency retains audit records for ninety (90) days and archive old records for ten (10) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and Agency information retention requirements.

AU-12: Audit Generation

Agency systems:

a. Provide audit record generation capability for the following auditable events defined in AU-2: Audit Events:
   - All successful and unsuccessful authorization attempts;
   - All changes to logical access control authorities (e.g., rights, permissions);
   - All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services;
   - The audit trail, which must capture the enabling or disabling of audit report generation services; and
   - The audit trail must capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).
b. Allows Security Operations Center personnel, Systems Administrator personnel, or other applicable personnel or roles to select which auditable events are to be audited by specific components of the information system; and
c. Generates audit records for the list of events defined in AU-2: Audit Events with the content defined in AU-3: Content of Audit Records.

AU-12 HIPAA mapping

45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b)

AU-16: Cross-Agency Auditing

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

AU-16 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b); 45 C.F.R. §164.314

AU-16 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, this requirement applies to outsourced data centers or cloud providers. The provider must be held accountable to protect and share audit information with the agency through the contract.

Assessment and Authorization

AIM 216 Minimum Protection Requirement for CA

The Agency will: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

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

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. Assessment, Authorization, & 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 Assessment, Authorization, & Monitoring policy and the associated Assessment, Authorization, & Monitoring controls;
b. Designates the Chief Information Security Officer to manage the Assessment, Authorization, & Monitoring policy and procedures;
c. Reviews and updates the current Assessment, Authorization, & Monitoring:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the Assessment, Authorization, & Monitoring procedures implement the Assessment, Authorization, & Monitoring policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the Assessment, Authorization, & Monitoring.

CA-1 HIPAA mapping

HIPAA: 164.308(a)(8) 45 C.F.R. §164.316(b)(1)(ii); 45 C.F.R. §164.316(b)(2)(ii); 45 C.F.R. §164.308(a)(2)

CA-2: Assessments

The agency:

a. Develops an information security and privacy control assessment plan that describes the scope of the assessment including:
    1. Security and privacy controls and control enhancements under assessment (including information security and privacy changes enacted by agency CIO/CISO directives).
    2. Assessment procedures to be used to determine control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities.
b. Ensure the assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

c. Assesses the security and privacy controls in the information system and its environment of operation within every three (3) years, at a rate of 1/3 of the controls per year, and continually as part of configuration management processes 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;
d. Produces an assessment report that documents the results of the assessment; and
e. Provides the results of the security and privacy control assessment within sixty (60) days after its completion to the Authorizing Official, Chief Information Officer, Chief Information Security Officer, Program Manager responsible for the system, and the Information Security Office Governance, Risk, & Compliance Management team.

CA-2 (enhancement 1): Independent Assessors

The agency employs assessors or assessment teams with agency CISO level of independence to conduct security control assessments.

CA-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(8)

CA-3: System Interconnections

The agency:

a. Authorizes connections from the information system to other information systems using Interconnection Security Agreements (ISA) or other comparable agreements (such as MOU/MOA, SLA, or specific contractual clause, so long as the appropriate interconnection detail is provided therein);
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated;
c. Reviews and updates the interconnection agreements no less often that once every year and/or whenever significant changes (that can affect the security state of the information system) are implemented that could impact the validity of the agreement as a verification of enforcement of security requirements; and
d. Only activates a system interconnection (including testing) when a signed interconnection agreement is in place.

CA-3 (enhancement 5): Restrictions on External Connections

The agency employs a deny-all, permit-by-exception, policy for allowing agency information systems to connect to external information systems, except for client workstations connecting to internet resources – which employs a permit-all, deny-by-exception policy.

CA-3 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.308(b)(4), 45 C.F.R. §164.314(a)(2)(ii); 45 C.F.R. §164.308(b)(3); 45 C.F.R. §164.504(e)(3); 45 C.F.R. §164.312(a)(1)

CA-5: Plan of Action & Milestones

The agency:

a. Develops a plan of action and milestones for the system to document the planned remedial actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones monthly based on the findings from control assessments, impact analyses, and continuous monitoring activities.

CA-5 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(2), 45 C.F.R. §164.308(a)(8)

CA-5 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the POA&M must be comprised of an all-inclusive tool or document for the agency to track vulnerabilities identified by the self-assessments, internal inspections, external audits and any other vulnerabilities identified for information systems that receive, process, store, or transmit FTI.

CA-6: Authorization

The agency:

a. Assigns a senior-level executive or manager as the authorizing official for the system and for any common controls inherited by the system;
b. Ensure that the authorizing official, before commencing operations:
    1. Authorizes the system for processing; and
    2. Authorizes the common controls inherited by the system; and
c. Updates the security authorization:
    - Within every three (3) years;
    - When significant changes are made to the system;
    - When changes in requirements result in the need to process data of a higher sensitivity;
    - When changes occur to authorizing legislation or federal requirements that impact the system;
    - After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and
    - Prior to expiration of a previous security authorization.

CA-6 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(2); 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.316(b)(2)(iii)

CA-7: Continuous Monitoring

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of the following metrics monitored based on the organization security goals and objectives:
    - Compliance Percentage
    - PoA&M items open & PoA&M items closed
    - Security Incidents opened & closed
    - Threats observed/stopped
    - Vulnerability metrics
b. Establishment of the following frequencies, to correlate with Configuration Management practices & accommodate the assessments (defined in CA-2: Assessments), for monitoring and ongoing assessment of security and privacy control effectiveness:
    - Review one-half (1/2) of minimum baseline controls annually;
    - Review all controls every two years;
    - Review potentially affected controls as part of the Configuration Management processes;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of the metrics define in CA-7a in accordance with the organizational continuous monitoring strategy;
e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of the organization and the information system to the Authorizing Official, Chief Information Officer, Chief Information Security Officer, Program Manager responsible for the system, and the Information Security Office Governance, Risk, & Compliance Management team monthly.

CA-7 (enhancement 1): Independent Assessment

The organization employs assessors or assessment teams with agency CISO level of independence to monitor the security controls in the information system on an ongoing basis.

CA-7 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.308(a)(5)(ii)(C)

CA-8: Penetration Testing

The organization conducts both internal and external penetration testing on moderate systems that either support critical business functions or are publicly accessible, annually or whenever there has been a significant change to the system. At a minimum, penetration testing will be conducted to determine:

a. How well the system tolerates real world-style attack patterns;

b. The likely level of sophistication an attacker needs to successfully compromise the system;
c. Additional countermeasures that could mitigate threats against the system; and
d. Defenders' ability to detect attacks and respond appropriately

CA-9: Internal System Connections

The agency:

a. Authorizes connections of the following internal information system components or classes of components to the information system:
    - Printers, scanners, Multi-function
    - Communications Equipment
    - Workstations in internal LANs
    - Servers in internal LANs
    - Hosts within the same zones when applicable; and
b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

CA-9 HIPAA mapping

45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(1)

Configuration Management

AIM 216 Minimum Protection Requirement for CM

The Agency will: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

CM-1: Configuration Management Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A 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. Designates the Chief Information Security Officer to manage the configuration management policy and procedures;
c. Reviews and updates the current configuration management:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the configuration management procedures implement the configuration management policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the configuration management policy.

CM-2: Baseline Configuration

The agency develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

CM-2 (enhancement 1): Reviews and Updates

The agency reviews and updates the baseline configuration of the information system:

a. At least annually;
b. When configuration settings change due to critical security patches, upgrades, and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components), major system changes/upgrades;
c. As an integral part of:
    1. information system component installations;
    2. upgrades; and
    3. updates to applicable governing standards; and

d. Supporting baseline configuration documentation to reflect ongoing implementation of operational baseline configuration updates, either directly or by policy.

CM-2 (enhancement 2): Automation support for accuracy and currency

The agency employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

CM-2 (enhancement 3): Retention of previous configurations

The agency retains older versions of baseline configurations of the information system as deemed necessary to support rollback.

CM-2 (enhancement 7): Configure Systems, Components, or Devices for High risk areas

The agency:

a. Issues dedicated information systems, system components, or devices (laptop, mobile device) with stringent configurations (e.g., FIPS 140-2 for encryption, CIS Benchmark Level 1) to individuals traveling to locations that the organization deems to be of significant risk; and
b. Applies security safeguards to the devices (i.e., detailed inspection of the device for physical tampering, purging or reimaging the hard disk drive/removable media, antivirus/antimalware scans, posture host for patch levels) when the individuals return.

CM-3: Configuration Change Control

The agency:

a. Determines the types of changes to the information system that are configuration-controlled;
b. Reviews, on an as-needed basis, but not less than quarterly, proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
c. Documents configuration change decisions associated with the information system;
d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system for a minimum of three (3) years after the change;
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for configuration change control activities through change request forms which must be approved by an organizational change control board that convenes frequently enough to accommodate proposed change requests, and other appropriate organizational officials as required including, but not limited to, the System Developer/Maintainer and Systems Administrators.

CM-3 (enhancement 2): Test/Validate/Document Changes

The agency tests, validates, and documents changes to the information system before implementing the changes on the operational system.

CM-3 (enhancement 4): Security Representative

The agency requires that a security representative be a member of each system's change control/authority or configuration management board.

CM-3 HIPAA mapping

45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(e)(2)(ii)

CM-4: Security & Privacy Impact Analyses

The organization analyzes changes to the information system to determine potential security and privacy impacts prior to change implementation.

CM-4 (enhancement 2): Separate Test Environments

The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

CM-5: Access Restrictions for Change

The agency defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

CM-6: Configuration Settings

The agency:

a. Establishes and documents configuration settings for components employed with the system using configuration settings established by the Information Security Office that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from the established configuration settings for all system components in production environments or that interact with production, unencrypted information based on acceptable risk levels as defined in the Agency's PM-32 Risk Frame or documented approval (in the PL-2 System Security Plan and/or change management processes) from the Information Owner, System Owner, Authorizing Official, and Information Security Office;
d. Monitors and controls changes to the configuration settings in accordance with the organizational policies and procedures.

CM-7: Least Functionality

The agency:

a. Configures the information system to provide only essential capabilities; and
b. Prohibits or restricts the use of high-risk, unnecessary, or insecure system services, ports, network protocols, and capabilities (e.g., Telnet, FTP, etc.) across network boundaries that are not explicitly required for system or application functionality.

CM-7 (enhancement 1): Periodic review

The agency:

a. Reviews the information system annually to identify and eliminate unnecessary functions, ports, protocols, and/or services;
b. Performs automated reviews of the information system annually to identify changes in functions, ports, protocols, and/or services; and
c. Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or insecure.

CM-7 (enhancement 2): Prevent Program Execution

Agency systems prevent program execution in accordance with policies regarding authorized software use which include, but are not limited to the following:

a. Software must be legally licensed;
b. Software must be supported;
c. Software must be provisioned in approved configurations; and
d. Users must be authorized for software program use.

CM-7 (enhancement 4): Unauthorized Software/Blacklisting

The agency:

a. Disallows unauthorized software programs to execute on the information system;
b. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system;
c. Reviews and updates the list of unauthorized software programs no less often than every seventy-two (72) hours; and
d. Receives automated updates from a trusted source.

CM-8: System Component Inventory

The agency:

a. Develops and documents an inventory of information system components that:
    1. Accurately reflects the current information system;
    2. Include all components within the authorization boundary of the information system;
    3. Are at the level of granularity deemed necessary for tracking and reporting; and
    4. Includes:

i. Each component's unique identifier and/or serial number;
ii. Information system of which the component is a part;
iii. Type of information system component (e.g., server, desktop, application);
iv. Manufacturer/model information;
v. Operating system type and version/service pack level;
vi. Presence of virtual machines;
vii. Application software version/license information;
viii. Physical location (e.g., building/room number);
ix. Logical location (e.g., IP address, position with the information system [IS] architecture);
x. Media access control (MAC) address;
xi. Ownership;
xii. Operational status;
xiii. Primary and secondary administrators; and
xiv. Primary user.

b. Reviews and updates the information system component inventory annually.

CM-8 (enhancement 1): Updates During Installations/Removals

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

CM-8 (enhancement 3): Automated Unauthorized Component Detection

The organization:

a. Employs automated mechanisms no less than weekly to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
b. Takes the following actions when unauthorized components and/or provisioned configurations are detected:
    1. Isolate the identified component;
    2. Notify the Security Operations Center;
    3. Notify Systems Administrators; and
    4. Notify the responsible actor(s) – the individual and/or the individual's supervisor

CM-8 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(d)(1), 45 C.F.R. §164.310(d)(2)(iii)

CM-9: Configuration Management Plan

The agency develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying and managing configuration items throughout the system development life cycle;
c. Defines the configuration items for the information system;

d. Places the configuration items under configuration management; and
e. Protects the configuration management plan from unauthorized disclosure and modification.

CM-10: Software Usage Restrictions

The agency:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents 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-10 (enhancement 1): Open Source Software

The Agency establishes the following restriction on the use of open source software:

Open source software must be:

- Legally licensed;
- Approved by the Agency IT department; and
- Adhere to a secure configuration baseline checklist that is approved by the CISO or his/her delegate.

CM-11: User-installed Software

The agency:

a. Prohibits the installation of software by users on agency owned and managed client devices unless approved by the agency CIO, a delegate of the CIO, or the agency CISO;
b. Enforces software installation policies through automated methods; and
c. Monitors policy compliance on a continual basis.

CM-12: Information Location

Agency systems:

a. Identify the location of sensitive or moderate categorized information and the specific system components on which the information resides;
b. Identify and document the users who have access to the system and the system components where the information resides; and
c. Document changes to the location where the information resides.

CM-12 (enhancement 1): AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION

Agency systems use automated tools to identify moderate or high categorized information and the specific system components on which the information resides to ensure adequate security and privacy controls are in place to protect organizational information and individual privacy.

Contingency Planning

AIM 216 Minimum Protection Requirement for CP

The Agency will establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations

CP-1: Contingency Planning Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A 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. Designates the Chief Information Security Officer to manage the contingency planning policy and procedures;
c. Reviews and updates the current contingency planning:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the contingency planning procedures implement the contingency planning policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the contingency planning policy.

CP-1 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(7)(i)

CP-2: Contingency Plan

The agency:

a. Develops a contingency plan using for each system that:
    1. Identifies essential missions & business functions and associated contingency requirements;
    2. Provides recovery objectives (recovery time objectives [RTO], recovery point objectives [RPO], and maximum tolerable downtimes [MTD]), 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 security and privacy controls originally planned and implemented; and
6. Is reviewed and approved by organizational leadership;

b. Distributes copies of the contingency plan to the Information Security Office, Program Manager, personnel coordinating the Contingency Plan, and other stakeholders identified within the contingency plan;
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews each system's contingency plan annually;
e. Updates 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. Communicates contingency plan changes to all parties involved in contingency plan activities; and
g. Protects the contingency plan from unauthorized disclosure and modification.

CP-2 (enhancement 1): Coordinate with related plans

The agency coordinates contingency plan development with organizational elements responsible for related plans.

CP-2 (enhancement 3): Resume essential missions and business functions

The agency plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions.

CP-2 (enhancement 8): Identify critical assets

The agency identifies critical system assets supporting essential missions & business functions.

CP-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.308(a)(7)(ii)(C), 45 C.F.R. §164.308(a)(7)(ii)(E), 45 C.F.R. §164.308(a)(7)(i)-(ii); 45 C.F.R. §164.310(a)(2)(i); 45 C.F.R. §164.312(a)(2)(ii)

CP-3: Contingency Training

The agency provides contingency training to operational and support personnel (including managers and information system users) consistent with assigned roles and responsibilities:

a. Within ninety (90) days of assuming a contingency role or responsibility;
b. When required by information system changes; and
c. Annually thereafter.

CP-3 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(D)

CP-4: Contingency Plan Testing

The agency:

a. Tests each system's contingency plan annually using functional exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective action if needed.

CP-4 (enhancement 1): Coordinate with related plans

The Agency coordinates contingency plan testing with organizational elements responsible for related plans.

CP-6: Alternate Storage Site

The agency:

a. Establishes an alternate storage site, including necessary agreements to permit the storage and retrieval of information system backup information; and
b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

CP-6 (enhancement 1): Separation from Primary site

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

CP-6 (enhancement 3): Accessibility

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-6 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.310(a)(2)(i)

CP-6 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will ensure that the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103.

CP-7: Alternate Processing Site

Agency systems:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of critical system operations for essential missions/business functions within the Maximum Tolerable Downtime (MTD) as specified by the system contingency plan or COOP

for the business function(s) supported by the system when the primary processing capabilities are unavailable;

b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the Maximum Tolerable Downtime (MTD) for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

CP-7 (enhancement 1): Separation from Primary Site

The agency identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

CP-7 (enhancement 2): Accessibility

The agency identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-7 (enhancement 3): Priority of Service

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organizational availability requirements (including recovery time objectives).

CP-7 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.310(a)(2)(i), 45 C.F.R. §164.308(7)(ii)(C)

CP-7 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will ensure that the alternate processing site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103.

CP-8: Telecommunication Services

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of critical system operations for essential mission and business functions within the Recovery Time Objectives (RTO) and Maximum Tolerable Downtime (MTD) when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8 (enhancement 1): Priority of Service Provisions

Agency systems:

a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives) for system operations in support of critical business functions; and

b. When applicable, request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

CP-8 (enhancement 2): Single Points of Failure

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

CP-8 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B)

CP-9: System Backup

The agency:

a. Conducts backups of user-level information contained in each system – weekly full & daily incremental/differential or according to the Recovery Point Objective (RPO) defined in the associated Contingency Plan, whichever is shorter;
b. Conducts backups of system-level information contained in each system – weekly full & daily incremental/differential or according to the Recovery Point Objective (RPO) defined in the associated Contingency Plan, whichever is shorter;
c. Conducts backups of system documentation including security-related documentation – weekly full; and
d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

CP-9 (enhancement 1): Testing for reliability and integrity

The agency tests its backup information semiannually (every 6 months) to verify media reliability and information integrity.

CP-9 (enhancement 8): Cryptographic protection

The agency implements cryptographic mechanisms to prevent unauthorized disclosure and modification of CP-9: System Backup data.

CP-9 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 45 C.F.R. §164.310(d)(2)(iv), 164.312(c)(1), 45 C.F.R. §164.308(a)(7)(ii)(C)

CP-9 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will protect the confidentiality of backup information at storage locations pursuant to IRC 6103 requirements.

CP-10: System Recovery and Reconstitution

The agency provides for the recovery and reconstitution of its systems to a known state after a disruption, compromise, or failure within the timeframes specified in the associated contingency plan.

CP-10 (enhancement 2): Transaction Recovery

The agency implements transaction recovery for systems that are transaction-based.

CP-10 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.308(a)(7)(ii)(C)

Identification and Authentication

AIM 216 Minimum Protection Requirement for IA

The Agency will identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

IA-1: Identification & Authentication Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. An Identification & 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 Identification & Authentication policy and the associated Identification & Authentication controls;
b. Designates the Chief Information Security Officer to manage the Identification & Authentication policy and procedures;
c. Reviews and updates the current Identification & Authentication:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the Identification & Authentication procedures implement the Identification & Authentication policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the Identification & Authentication policy.

IA-1 HIPAA mapping

HIPAA: 45 C.F.R. § 164.308(a)(5)(ii)(D); 45 C.F.R. § 164.312(a)(2)(i); 45 C.F.R. § 164.312(a)(2)(iii); 45 C.F.R. § 164.312(d)

IA-2: Identification & Authentication (Organizational Users)

The agency uniquely identifies and authenticates organizational users or processes acting on behalf of organizational users.

IA-2 (enhancement 1): Multifactor Authentication to privileged accounts

The Agency implements multifactor authentication for access to privileged accounts.

IA-2 (enhancement 2): Multifactor Authentication to non-privileged accounts

The Agency implements multifactor authentication for remote access to non-privileged accounts.

IA-2 (enhancement 8): Access to Accounts – Replay Resistant

The agency implements replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.

IA-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D), 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d)

IA-2 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency implements multi-factor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

IA-3: Device Identification & Authentication

Agency systems uniquely identify and authenticate specific or types of devices, as specified in the applicable System Security Plan, before establishing local, remote, or network connections.

IA-3 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(a)(1)

IA-4: Identifier Management

The agency manages information system identifiers by:

a. Receiving authorization from Agency Systems Administrators to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group, role, or device;
d. Preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of three (3) years or more has passed; and
e. Disabling the identifier after 60 days of inactivity.

IA-3 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d); 45 C.F.R. §164.308(a)(4); 45 C.F.R. §164.308(a)(5)(ii)(D)

IA-5: Authenticator Management

The agency manages system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the 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/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators as follows:
    - Passwords are valid for no longer than the period directed in IA-5(1), immediately in the event of known or suspected compromise, and immediately upon system installation (e.g. default or vendor-supplied passwords);
    - PIV compliant access cards are valid for no longer than five (5) years;
    - PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years; and
    - Any PKI authentication request must be validated by Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) to ensure that the certificate being used for authentication has not been revoked.
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes.

IA-5 (enhancement 1): Password-based authentication

For password-based authentication, the agency:

a) Enforces minimum password complexity of at least one character from each of the four character categories (A-Z, a-z, 0-9, special characters) with a length of 8 characters for non-privileged accounts and 15 characters for privileged accounts;
b) Enforces at least a minimum of six (6) characters change when new passwords are created;
c) Stores and transmits only cryptographically-protected passwords;
d) Enforces password minimum and maximum lifetime restrictions of one (1) day for the minimum, and sixty (60) days for a user account and one hundred eighty (180) days for a system/service account maximum;
e) Prevents password reuse for 24 generations;
f) Allows the use of a temporary password for system logons with an immediate change to a permanent password;
g) Employs automated tools to assist the user in selecting strong password authenticators; and
h) Prohibits the use of dictionary names or words.

IA-5 (enhancement 2): Public key-based authentication

For public key-based authentication, the agency:

a) Enforces authorized access to the corresponding private key; and

b) Maps the authenticated identity to the account of the individual or group; and when public-key infrastructure is used;
c) Validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; and
d) Implements a local cache of revocation data to support path discovery and validation.

IA-5 (enhancement 3): In-Person or Trusted Third-party Registration

The organization requires that the registration process to receive hardware administrative tokens and credentials used for two (2)-factor authentication be conducted in person before a designated registration authority with authorization by the Information Security Office.

IA-5 (enhancement 6): Protection of Authenticators

The agency protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

IA-5 (enhancement 11): Hardware Token-Based Authentication

For hardware token-based authentication, Agency systems use PKI certificates issued by globally/publicly recognized Certificate Authorities or a private, centrally managed Certificate Authority within the organization's IT environment.

IA-5 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3); 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R. §164.312(d)

IA-6: Authenticator Feedback

Agency systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

IA-6 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R. §164.312(a)(1)

IA-7: Cryptographic Module Authentication

Agency systems implement mechanisms for authentication to a cryptographic module that meet the requirements of FIPS 140-2, and when applicable, other federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

IA-7 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R.§164.312(a)(2)(iv)

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

Agency systems uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users) prior to gaining access to agency systems and networks.

IA-8 HIPAA mapping

45 C.F.R. §164.312(a)(2)(i)

Incident Response

AIM 216 Minimum Protection Requirement for IR

The Agency will: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

IR-1: Incident Response Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. An 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. Designates the Chief Information Security Officer to manage the Incident Response policy and procedures;
c. Reviews and updates the current Incident Response:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the Incident Response procedures implement the Incident Response policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the Incident Response policy.

IR-1 HIPAA mapping

HIPAA: 45 C.F.R.§164.308(a)(6)(i); 45 C.F.R. §164.530(b)(1)

IR-2: Incident Response Training

The agency provides incident response training to information system users consistent with assigned roles and responsibilities:

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

IR-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(6)(i)

IR-3: Incident Response Testing

The agency tests the Incident Response capability for each of its systems annually using checklists, walk-through/tabletop exercises, parallel and full-interrupt simulations, and comprehensive exercises to determine the incident response effectiveness and documents the results.

IR-3 (enhancement 2): Coordination with Related Plans

The agency coordinates incident response testing with organizational elements responsible for related plans.

IR-3 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(6)(i)

IR-3 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency:

a. Performs tabletop exercises using scenarios that include a breach of FTI and should test the agency's incident response policies and procedures.
b. Includes a subset of all employees and contractors with access to FTI in tabletop exercises.
c. Produces an after-action report to improve existing processes, procedures, and policies as a part of each tabletop exercise.

IR-4: Incident Handling

The agency:

a. Implements an incident handling capability for security and privacy incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities;
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly; and
d. Ensures the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

IR-4 (enhancement 1): Automated Incident Handling Processes

The agency employs automated mechanisms to support the incident handling process.

IR-4 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(6)(ii); 45 C.F.R. Part 164 Subpart D

IR-5: Incident Monitoring

The organization tracks and documents all physical, information security, and privacy incidents.

IR-5 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(6)(ii); 45 C.F.R. Part 164 Subpart D

IR-6: Incident Reporting

The agency:

a. Requires personnel to report actual or suspected security and privacy incidents to the agency helpdesk or Security Operations Center and the Privacy Office immediately upon discovering a suspected security incident; and
b. Reports security incident information to authorities defined in the Incident Response plan.

IR-6 (enhancement 1): Automated Reporting

The agency employs automated mechanisms to assist in the reporting of security incidents.

IR-6 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(6)(ii), 45 C.F.R. §164.314(a)(2)(i); 45 C.F.R. §164.314(a)(2)(i)(C); 45 C.F.R. Part 164 Subpart D

IR-6 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will meet the requirements of Section 10.0, Reporting Improper Inspections or Disclosures, which includes contacting the appropriate special agent-in-charge, TIGTA, and the IRS Office of Safeguards immediately but no later than 24 hours after identification of a possible issue involving FTI.

IR-7: Incident Response Assistance

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

IR-7 (enhancement 1): Automation Support for Availability of Information/Support

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

IR-7 HIPAA mapping

HIPAA: 164.308(a)(6)(ii)

IR-8: Incident Response Plan

The agency:

a. Develops 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. Is reviewed and approved by the Chief Information Officer biennially; and
    9. Explicitly designates the responsibility for incident response to the AMA Information Security Office Security Operations Center.
b. Distributes copies of the incident response plan to all parties involved in the Incident Response process, including organizational leadership;
c. Updates the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
d. Communicates incident response plan changes to all parties involved in the Incident Response process,
e. Protects the Incident Response plan from unauthorized disclosure and modification.

IR-8 HIPAA mapping

45 C.F.R. §164.308(a)(6) C.F.R

IR-9: Information Spillage Response (Additional IRS 1075 Requirements)

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency must respond to information spills by:

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

System Maintenance

AIM 216 Minimum Protection Requirement for MA

The Agency will: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

MA-1: Incident Response Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A 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. Designates the Chief Information Security Officer to manage the System Maintenance policy and procedures;
c. Reviews and updates the current System Maintenance:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the System Maintenance procedures implement the System Maintenance policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the System Maintenance policy.

MA-2: Controlled Maintenance

The agency:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on-site or removed to another location;
c. Requires that the applicable System Owner, or other applicable official, explicitly approves the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
f. Includes required maintenance-related information in organizational maintenance records.

MA-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(a)(2)(iv); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(d)(2)(iii)

MA-3: Maintenance Tools

The organization approves, controls, and monitors information system maintenance tools.

MA-3 (enhancement 1): Inspect Tools

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

MA-3 (enhancement 2): Inspect Media

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

MA-3 (enhancement 3): Prevent Unauthorized Removal

The agency prevents the unauthorized 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, in writing, from the agency CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.

MA-4: Nonlocal Maintenance

The agency:

a. Approves and continuously monitors nonlocal maintenance and diagnostic activities;
b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
c. Employs strong identification and authentication techniques in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintains records for nonlocal maintenance and diagnostic activities; and
e. Terminates all sessions and network connections when nonlocal maintenance is completed.

MA-4 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(1); 45 C.F.R. §164.312(e)(2)(ii)

MA-4 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency Documents policies and procedures for the establishment and use of non-local maintenance and diagnostic connections.

MA-5: Maintenance Personnel

The agency:

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

MA-5 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(a)(2)(iv); 45 C.F.R. §164.310(d)(2)(iii)

MA-6: Timely Maintenance

The organization obtains maintenance support and/or spare parts for information system components supporting critical business functions within the applicable Recovery Time Objective (RTO) specified in the contingency plan.

MA-6 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(a)(2)(iv)

Media Protection

AIM 216 Minimum Protection Requirement for MP

The Agency will: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

MP-1: Media Protection Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A 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. Designates the Chief Information Security Officer to manage the Media Protection policy and procedures;
c. Reviews and updates the current Media Protection:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the Media Protection procedures implement the Media Protection policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the Media Protection policy.

MP-2: Media Access

The agency restricts access to sensitive digital and non-digital media to System Administrators, Business roles requiring access, and other agency personnel as required.

MP-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 164.312(c)(1); 45 C.F.R. §164.310(c); 45 C.F.R. §164.310(d)(1)

MP-3: Media Marking

The agency:

a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempts specific types of media or hardware components from marking if the media remains within a secure environment.

MP-3 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency must label removable media (CDs, DVDs, diskettes, magnetic tapes, external hard drives and flash drives) and information system output containing FTI (reports, documents, data files, back-up tapes) indicating "Federal Tax Information". Notice 129-A and Notice 129-B IRS provided labels can be used for this purpose.

MP-4: Media Storage

The agency:

a. Physically controls and securely stores digital and non-digital media containing sensitive information within controlled areas; and
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

MP-4 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(c), 45 C.F.R. §164.310(d)(1), 45 C.F.R. §164.310(d)(2)(iv)

MP-4 Additional IRS 1075 requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will meet the additional secure storage requirements listed in Section 4.0, Secure Storage—IRC 6103(p)(4)(B) of IRS Publication 1075.

MP-5: Media Transport

The agency:

a. Protects and controls digital and non-digital media containing sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging, and:
    1. if hand carried, using a securable container (e.g., locked briefcase) via authorized personnel, or
    2. if shipped, trackable with receipt by commercial carrier.
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of information system media; and
d. Restricts the activities associated with the transport of information system media to authorized personnel.

MP-5 (enhancement 4):

Agency systems implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

MP-5 HIPAA mapping

45 C.F.R. §164.312(a)(2)(iv)

MP-5 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will meet the media transport requirements listed in Section 4.4, FTI in Transit of IRS Publication 1075.

MP-6: Media Sanitization

The agency:

a. Sanitizes system media, including hard copy media, prior to disposal, release out of organizational control, or release for reuse using purging, destroying, cryptographic erase (per NIST 800-88r1) in accordance with applicable federal and organizational standards and policies; and
b. Employs the purging, destroying, cryptographic erase (per NIST 800-88r1) sanitization techniques with the strength and integrity commensurate with the security category or classification of the information.

MP-6 (enhancement 1): Review, Approve, Track, Document, and Verify

The Agency reviews, approves, tracks, and verifies media sanitization and disposal actions.

MP-6 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(d)(1), 45 C.F.R. §164.310(d)(2)(i); 45 C.F.R. §164.310(d)(2)(iii), 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.312(d)(2)(ii)

MP-6 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will meet the media sanitization requirements listed in Section 9.4.7, Media Sanitization of IRS Publication 1075.

MP-7: Media Use

The agency restricts the use of personally owned and portable media on user workstations and user mobile devices on user workstations and user mobile devices.

MP-7 (enhancement 1): Prohibit Use without owner

The agency prohibits the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Physical and Environmental

AIM 216 Minimum Protection Requirement for PE

The Agency will: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

PE-1: Physical & Environmental Protection Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A Physical & 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 & Environmental Protection policy and the associated Physical & Environmental Protection controls;
b. Designates the Chief Information Security Officer to manage the Physical & Environmental Protection policy and procedures;
c. Reviews and updates the current Physical & Environmental Protection:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the Physical & Environmental Protection procedures implement the Physical & Environmental Protection policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the Physical & Environmental Protection policy.

PE-1 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.310(a)(2)(ii), 45 C.F.R. §164.310(a)(2)(iii)

PE-2: Physical Access Authorizations

The agency:

a. Develops, approves, and maintains lists of individuals with authorized access to facilities where agency systems reside;
b. Issues authorization credentials for facility access;
c. Reviews the access lists detailing authorized facility accesses by individuals every 6 months; and
d. Removes individuals from the facility access lists when access is no longer required.

PE-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii)

PE-2 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will enforce physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where FTI is received, processed, stored, or transmitted

PE-3: Physical Access Control

The agency:

a. Enforces physical access authorizations at all entry and exit points to the facilities where systems reside by:
    - Verifying individual access authorizations before granting access to the facility; and
    - Controlling ingress and egress to the facility using physical access control systems/devices and/or guards;
b. Maintains physical access audit logs for all public entry and exit points;
c. Provides physical access control systems/devices and guards to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity while inside areas not officially designated as publicly accessible;
e. Secures keys, combinations, and other physical access devices;
f. Inventories physical access devices, such as keys, badges/cards, card readers, and locks biennially;
g. Changes:
    - Combinations – annually, when compromised, or when individuals using the combination are transferred or terminated
    - Keys - when keys are lost or compromised/improperly duplicated

PE-3 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.310(b)

PE-4: Access Control for Transmission

The agency controls physical access to telephone closets and information system distribution and transmission lines within organizational facilities using physical/key locks, cameras, and/or locking equipment racks.

PE-4 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(a)(2)(ii); 45 C.F.R. §164.310(c)

PE-5: Access Control for Output Devices

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

PE-5 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.310(b), 164.310(c)

PE-6: Monitoring Physical Access

The agency:

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access logs monthly and upon occurrence of security incidents or indications of potential events involving physical security; and
c. Coordinates results of reviews and investigations with the organization's incident response capability.

PE-6 (enhancement 1): Intrusion Alarms/Surveillance Equipment

The organization monitors physical intrusion alarms and surveillance equipment.

PE-6 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.308(a)(6)(i)

PE-8: Visitor Access Records

The agency:

a. Maintains visitor access records to the facility where the information system resides for five (5) years; and
b. Reviews visitor access records no less often than monthly.

PE-8 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will meet visitor access requirements listed in Section 4.3 Restricted Area Access of IRS Publication 1075.

PE-9: Power Equipment and Cabling

The agency protects power equipment and power cabling for the information system from damage and destruction.

PE-10: Emergency Shutoff

The agency:

a. Provides the capability of shutting off power within data centers to the information system or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.

PE-11: Emergency Power

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to a long-term alternate power source in the event of a primary power source loss.

PE-12: Emergency Lighting

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility.

PE-13: Fire Protection

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

PE-13 (enhancement 3): Automatic Fire Suppression

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

PE-14: Temperature and Humidity Controls

The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-specified levels;
b. Monitors temperature and humidity level regularly; and
c. Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three (3) years.

PE-15: Water Damage Protection

The agency protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

PE-16: Delivery and Removal

The agency authorizes, monitors, and controls the flow of all information system-related components entering and exiting the facility and maintains records of those items.

PE-17: Alternate Work Site

The agency:

a. Employs information security safeguards equivalent to that of the primary site security controls at alternate work sites;
b. Assesses, as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

PE-17 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(a)(2)(i)

PE-17 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will meet the requirements listed in Section 4.7 Telework Locations for off-site locations such as other government facilities or private residences of employees.

PE-18: Location of Information System Components (Additional IRS 1075 Requirements)

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Planning

AIM 216 Minimum Protection Requirement for PL

The Agency will develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

PL-1: Planning Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A Security 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 Security Planning policy and the associated Planning controls;
b. Designates the Chief Information Security Officer to manage the Security Planning policy and procedures;
c. Reviews and updates the current Security Planning:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the Security Planning procedures implement the Security Planning policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the Security Planning policy.

PL-1 HIPAA mapping

HIPAA: 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(i); 45 C.F.R. §164.316(b)(2)(ii)

PL-2: System Security Plan

The agency:

a. Develops security and privacy plans for agency systems that:
    1. Are consistent with the organization's Enterprise Architecture;
    2. Explicitly define the authorization boundary for the system;
    3. Describe the operational context of the system in terms of missions and business processes;
    4. Provide the security categorization of the system including supporting rationale;
    5. Describe the operational environment for the system and relationships with or connections to other systems;
    6. Provide an overview of the security and privacy requirements for the system;

7. Identify any relevant overlays, if applicable;
8. Describe the security and privacy controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
9. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security and privacy plans and communicate subsequent changes to the plans to the Authorizing Official, Information Owner, System Owner, Chief Information Officer, Chief Information Security Officer, and other applicable personnel or roles;
c. Reviews the security and privacy plans every three years;
d. Updates the security and privacy plans, minimally every three (3) years, to address current conditions or whenever:
    - There are significant changes to the information system/environment of operation that affect security;
    - Problems are identified during plan implementation or security control assessments;
    - When the data sensitivity level increases;
    - After a serious security violation caused by changes in the threat environment; or
    - Before the previous security authorization expires.
e. Protects the security and privacy plans from unauthorized disclosure and modification.

PL-2 (enhancement 3): Plan and Coordinate with Other Organizational Entities

The Agency plans and coordinates security and privacy related activities affecting the system with the Information Owner, System Owner, Chief Information Officer, Chief Information Security Officer, and other applicable personnel or roles before conducting such activities to reduce the impact on other organizational entities.

PL-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.306(a); 45 C.F.R. §164.308(a)(1)(i); 45 C.F.R. §164.310; 45 C.F.R. §164.310(a)(2)(ii); 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(ii)

PL-2 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency will, in addition to the agency System Security Plan,:

a. Develop an SSR to include information systems that:
    1. Is consistent with the agency's safeguarding requirements
    2. Explicitly defines the information systems that receive, process, store, or transmit FTI
    3. Describes the operational context of the information system in terms of missions and business processes
    4. Describes the operational environment for the information system and relationships with or connections to other information systems
    5. Provides an overview of the security requirements for the system
    6. Identifies any relevant overlays, if applicable
    7. Describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring and supplementation decisions

8. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation

b. Distribute copies of the SSR and communicate subsequent changes to the SSR to designated agency officials and the Office of Safeguards.
c. Review the SSR for the information system on an annual basis.
d. Update the SSR to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
e. Protect the SSR from unauthorized disclosure and modification.

PL-4: Rules of Behavior

The organization:

a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior regarding information and information system usage;
b. Receives an acknowledgment 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. Reviews and updates the rules of behavior annually; and
d. Requires individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules of behavior are revised/updated and at least annually;

PL-4 (enhancement 1): Social Media and Networking Restrictions

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

PL-4 Additional IRS 1075 Requirements

The agency prohibits, and makes explicit this prohibition in each applicable system's Rules of Behavior, the sharing of Federal Tax Information using any social media/networking sites.

PL-8: Security and Privacy Architectures

The agency:

a. Develops an information security architecture for the information system that:
    1. Describes the overall requirements and approach to be taken regarding protecting the confidentiality, integrity, and availability of organizational information;
    2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
    3. Describes any information security assumptions about, and dependencies on, external services.
b. Reviews and updates (as necessary) the information security architecture no less often than every three (3) years and whenever changes are made to the enterprise architecture;

c. Reflects planned security and privacy architecture changes in the security and privacy plans, the Concept of Operations (CONOPS), and organizational procurements and acquisitions.

PL-10: Baseline Selection

The agency selects a control baseline for each of its systems.

PL-11: Baseline Tailoring

The agency tailors the selected control baseline by applying specified tailoring actions.

Personnel Security

AIM 216 Minimum Protection Requirement for PS

The Agency will: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

PS-1: Personnel Security Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A 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. Designates the Chief Information Security Officer to manage the Personnel Security policy and procedures;
c. Reviews and updates the current Personnel Security:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the Personnel Security procedures implement the Personnel Security policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the Personnel Security policy.

PS-1 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(C); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(ii)

PS-2: Position Risk Designation

The agency:

a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions;
c. Reviews and, if necessary, updates position risk designations at least annually or whenever a position's duties are changed/revised/realigned.

PS-3: Personnel Screening

The organization:

a. Screens individuals prior to authorizing access to the information system;
b. Rescreens individuals every 10 years and anytime the individual moves to a new position with a higher risk designation.

PS-3 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency meets the requirements listed in Section 5.1.1 Background Investigation Minimum Requirements of IRS Publication 1075.

PS-4: Personnel Termination

The agency, upon termination of individual employment:

a. Disables information system access prior to or during the employee termination process;
b. Terminates/revokes any authenticators/credentials associated with the individual;
c. Conducts exit interviews that include a discussion of non-disclosure of sensitive information, information security, and privacy information;
d. Retrieves all security-related organizational information system-related property;
e. Retains access to organizational information and information systems formerly controlled by the terminated individual; and
f. Notifies the individual's chain of command, Human Resources, Helpdesk, the Information Security Office, and other applicable personnel and roles within one (1) calendar day.

PS-5: Personnel Transfer

The agency:

a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiates transfer or reassignment actions during or immediately after the formal transfer process.
c. Modifies access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notifies the individual's chain of command, Human Resources, Helpdesk, the Information Security Office, and other applicable personnel and roles within one (1) calendar day.

PS-5 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(C); 45 C.F.R. §164.308(a)(3)(ii)(B)

PS-6: Access Agreements

The agency:

a. Develops and documents access agreements for organizational systems;
b. Reviews and updates the access agreements annually; and
c. Verifies that individuals requiring access to organizational information systems:
    1. Acknowledge appropriate access agreements prior to being granted access; and
    2. Re-acknowledge access agreements to maintain access to organizational systems when access agreements have been updated and/or annually.

PS-6 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(B), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(d)(2)(iii), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii); 45 C.F.R. §164.314(a)

PS-7: External Personnel Security

The agency:

a. Establishes personnel security requirements including security roles and responsibilities for third-party (e.g. external, contractor or cloud service provider [CSP]) providers;
b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
c. Documents personnel security requirements;
d. Requires third-party providers to notify Contracting Officers and other agency contacts of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges as soon as possible within a maximum of three days, from the formal termination or transfer action; and
e. Monitors provider compliance.

PS-7 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii); 45 C.F.R. §164.314(a)

PS-8: Personnel Sanctions

The agency:

a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies the individual's chain of command, Human Resources, Helpdesk, the Information Security Office, and other applicable personnel and roles within seven calendar days when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

PS-8 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(C)

Risk Assessment

AIM 216 Minimum Protection Requirement for RA

The Agency will periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

RA-1: Risk Assessment Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A 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;
b. Designates the Chief Information Security Officer to manage the Risk Assessment policy and procedures;
c. Reviews and updates the current Risk Assessment:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the Risk Assessment procedures implement the Risk Assessment policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the Risk Assessment policy.

RA-1 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.514(d)(1)-(5)

RA-2: Security Categorization

The agency:

a. Categorizes its systems and the information it processes, stores, and transmits;
b. Documents the security categorization results, including supporting rationale, in the security plan for the system; and
c. Verifies that the authorizing official or authorizing official's designated representative reviews and approves the security categorization decision.

RA-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(A), 45 C.F.R. §164.308(a)(1)(ii)(B), 45 C.F.R. §164.308(a)(7)(ii)(E)

RA-3: Risk Assessment

The agency:

a. Conducts a risk assessment, including the likelihood and magnitude of harm, from:
    1. The unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
    2. Privacy-related problems for individuals arising from the intentional processing of personally identifiable information;
b. Integrates risk assessment results and risk management decisions from the organization and mission/business process perspectives with system-level risk assessments;
c. Documents risk assessment results in security and privacy plans, risk assessment reports, and plans of action and milestones;
d. Reviews risk assessment results within 1 year of the assessment
e. Disseminates risk assessment results to the Authorizing Official, Program Managers (as related to the scope of the risk assessment), the Chief Information Security officer, the Chief Information Officer, and other affected stakeholders as necessary;
f. Updates the risk assessment every two 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.

RA-3 HIPAA mapping

HIPAA: 45 C.F.R. §164.316(a), 164.308(a)(1)(ii)(A), 45 C.F.R. §164.308(a)(1)(ii)(B)

RA-5: Vulnerability Scanning

The agency:

a. Scans for vulnerabilities in its systems and hosted applications at least monthly, randomly, or when new vulnerabilities potentially affecting systems are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automates parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures;
    3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from control assessments'
d. Remediates legitimate vulnerabilities within 30 days for high or critical vulnerabilities, 60 days for moderate vulnerabilities, and 180 days for low vulnerabilities in accordance with an organizational assessment of risk;
e. Shares information obtained from the vulnerability scanning process and control assessments with Authorizing Officials, Information Owners, System Owners, the Chief Information Officer, and the Chief Information Security Officer to help eliminate similar vulnerabilities in other systems; and

f. Employs vulnerability scanning tools that include the capability to readily update the vulnerabilities to be scanned.

RA-5 (enhancement 2): Update by Frequency, Prior to New Scan, or When Identified

The agency updates the system vulnerabilities to be scanned daily and when new vulnerabilities are identified or reported.

RA-5 (enhancement 5): Privileged Access

The agency implements privileged access authorization to operating system, telecommunications, and subsystem components for patch-level and configuration vulnerability scanning activities to facilitate more thorough scanning.

RA-5 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(1)(i), 45 C.F.R. §164.316(a)

System and Services Acquisitions

AIM 216 Minimum Protection Requirement for SA

The Agency will: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

SA-1: System & Services Acquisition Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A System & 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 & Services Acquisition policy and the associated System & Services Acquisition controls;
b. Designates the Chief Information Security Officer to manage the System & Services Acquisition policy and procedures;
c. Reviews and updates the current System & Services Acquisition:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the System & Services Acquisition procedures implement the System & Services Acquisition policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the System & Services Acquisition policy.

SA-2: Allocation of Resources

The agency:

a. Determines information security requirements for the information system or information system service in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process;
c. Includes information security requirements in mission/business case planning, and
d. Establishes a discrete line item in organizational programming and budgeting documentation for the implementation and management of information systems security.

SA-3: System Development Lifecycle

The agency:

a. Manages its systems using System Development Life Cycles that incorporate information security and privacy considerations;
b. Defines and documents information security and privacy roles and responsibilities throughout the system development life cycles;
c. Identifies individuals having information security and privacy roles and responsibilities; and
d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

SA-3 (enhancement 2): Use of Live Data

The agency:

a. Approves, Documents, and controls the use of live data in development, test, and integration environments for its systems, systems components, or system services; and
b. Ensures development, test, and integration environments for systems, system components, or system services are protected at the same impact or classification level as any live data used.

SA-4: Acquisition Process

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

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

SA-4 (enhancement 1): Functional Properties of Security Controls

The agency requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

SA-4 (enhancement 2): Design/Implementation Information for Security Controls

The agency requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes:

a. Security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces;
b. Source code and hardware schematics; and
c. High-level design documentation at sufficient detail to prove the security control implementation.

SA-4 (enhancement 9): Functions/Ports/Protocols/Services in Use

The agency requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

SA-4 HIPAA Mapping

HIPAA: 164.314(a)(2)(i); 45 C.F.R. §164.314(a)

SA-5: System Documentation

The agency:

a. Obtains administrator documentation for the information system, system component, or information system service that describes:
    1. Secure configuration, installation, and operation of the system, component, or service;
    2. Effective use and maintenance of security functions/mechanisms; and
    3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
b. Obtains user documentation for the information system, system component, or information system service that describes:
    1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
    2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
    3. User responsibilities in maintaining the security of the system, component, or service;
c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent, and evaluate whether such documentation is essential for the effective implementation or operation of security controls;
d. Protects documentation as required, in accordance with the risk management strategy; and
e. Distributes documentation to development team, team leadership, system owner, information owner, and other individuals and roles as required.

SA-8: Security and Privacy Engineering Principles

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

SA-9: External System Services

The agency:

a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents governance oversight and user roles and responsibilities regarding external information system services in a SLA or similar agreement; and
c. Employs processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

SA-9 (enhancement 2): Identification of Functions/Ports/Protocols/Services

The organization requires providers of external information system services that store, process, or transmit sensitive agency information to identify the functions, ports, protocols, and other services required for the use of such services.

SA-9 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency restricts the location of information systems that receive, process, store, or transmit FTI to areas within the United States territories, embassies, or military installations.

Additionally, the agency prohibits the use of non-agency-owned information systems, system components, or devices that receive, process, store, or transmit FTI unless explicitly approved by the Office of Safeguards using the notification requirements listed in Section 7.4.5 Non-Agency-Owned Information Systems of IRS Publication 1075.

Contracts written for agency contracted systems that receive, process, store, transmit, or dispose of Federal Tax Information must contain IRS Publication 1075 Exhibit 7 language as well as meet the requirements listed in Section 9.3.15.4 Acquisition Process of IRS Publication 1075.

SA-9 HIPAA mapping

HIPAA: 45 C.F.R. §164.530; 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.308(b)(4), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii)

SA-10: Developer Configuration Management

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

a. Perform configuration management during system, component, or service development, implementation, and operation;
b. Document, manage, and control the integrity of changes to 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 impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to the Information Security Office, Chief Information Officer, program manager, system owner, information owner, and other individuals and roles as required.

SA-11: Developer Security Testing and Evaluation

The organization requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan in accordance with, but not limited to, current organizational procedures;
b. Perform regression testing/evaluation at high level design depth and coverage;
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during security testing/evaluation.

SA-15: Development Process, Standards, and Tools

The agency:

a. Requires developers of systems, system components, or system services to follow a documented development process that:
    1. Explicitly addresses security 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. Reviews the development process, standards, tools, tool options, and tool configurations.

SA-15 (enhancement 9): Use of Live Data

The organization disallows use of live data in development and test environments for the information system, system component, or information system service without prior approval of the Authorizing Official (AO).

SA-22: Unsupported System Components

The agency:

a. Replaces information system components as soon as possible after discovery that support for the components is no longer available from the developer, vendor, or manufacturer, and
b. Where immediate replacement is not possible, provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

SA-22 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, without exception, the agency must replace information system components (specifically security patches and/or product updates) when support for the components is no longer available from the developer, vendor, or manufacturer.

System and Communications Protection

AIM 216 Minimum Protection Requirement for SC

The Agency will: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response

SC-1: System and Communications Protection Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A 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. Designates the Chief Information Security Officer to manage the System and Communications Protection policy and procedures;
c. Reviews and updates the current System and Communications Protection:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the System and Communications Protection procedures implement the System and Communications Protection policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the System and Communications Protection policy.

SC-2: Application Partitioning

Agency systems separate user functionality (including user interface services) from information system management functionality.

SC-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(a)(1)

SC-4: Information in Shared Systems Resources

Agency systems prevent unauthorized and unintended information transfer via shared system resources.

SC-4 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(a)(1)

SC-5: Denial of Service Protection

Agency systems protect against or limit the effects of denial of service attacks such as:

- Distributed Denial of Service
- TCP SYN Flood
- Teardrop attack
- Low-rate DOS
- ICMP flood
- HTTP flood
- Other prolific DOS attack types

SC-7: Boundary Protection

The agency:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and
c. Connects to external networks or systems through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

SC-7 (enhancement 3): Access Points

The agency limits the number of external connections to its systems.

SC-7 (enhancement 4): External Telecommunications Services

The agency:

a. Implements a managed interface for each of external telecommunication service;
b. Establishes a traffic flow policy for each managed interface;
c. Protects the Confidentiality and Integrity of the information being transmitted across each interface;
d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
e. Reviews exceptions to the traffic flow policy annually and removes exceptions that are no longer supported by an explicit mission/business need.

SC-7 (enhancement 5): Deny by Default – Allow by Exception

Agency systems, at managed interfaces, deny network communications traffic by default and allow network communications traffic by exception.

SC-7 (enhancement 7): Prevent Split Tunneling for Remote Devices

Agency systems, in conjunction with a remote device, prevent the remote device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

SC-7 (enhancement 8): Route Traffic to Authenticated Proxy Servers

Agency systems route all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at managed interfaces.

SC-7 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(e)(1); 45 C.F.R. §164.312(e)(2)(i)

SC-7 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency meets the requirements as listed in Section 9.4.10 Network Protections of IRS Publication 1075.

SC-8: Transmission Confidentiality & Integrity

Agency systems protect the confidentiality and integrity of transmitted information.

SC-8 (enhancement 1): Cryptographic Protection

Agency systems implement FIPS 140-2 compliant cryptographic mechanisms to prevent the unauthorized disclosure of information and detect changes to information during transmission across wide area and local area transmissions.

SC-8 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.312(c)(2), 45 C.F.R. §164.312(e)(2)(i); 45 C.F.R. §164.312(e)(1)

SC-10: Network Disconnect

Agency systems:

a. terminate the network connection associated with a communications session at the end of the session, or:
    1. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and
    2. Forcibly disconnects:
        i. inactive remote client-based connections (including VPN connections) after thirty (30) minutes or less of inactivity,
        ii. inactive communications sessions (including stateful firewall sessions) after 60 minutes, and

b. Terminate or suspend network connections (i.e., a system to system interconnection) upon issuance of an order by the agency Commissioner, Authorizing Official, CIO, CISO, or Privacy Officer.

SC-10 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(B)

SC-12: Cryptographic Key Establishment and Management

The agency systems establish and manage cryptographic keys for required cryptography employed within the information system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

SC-13: Cryptographic Protection

Agency systems implement, for sensitive information, FIPS-validated cryptography or other laws, Executive Orders, directives, policies, regulations, and standards as applicable.

SC-15: Collaborative Computing Devices and Applications

The Agency:

a. Prohibits remote activation of collaborative computing devices except where explicitly permitted by the Authorizing Official or CIO; and
b. Provides an explicit indication of use to users physically present at the devices.

SC-15 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, or when Federal Tax Information is discussed over Collaborative Computing Devices and Applications, the agency:

- Prohibits remote activation of collaborative computing devices; and
- Provides an explicit indication of use to users physically present at the devices.

SC-17: Public Key Infrastructures

The agency issues public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider.

SC-18: Mobile Code

The organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

SC-19: Voice Over Internet Protocol

The agency:

a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously;
b. Authorizes, monitors, and controls the use of VoIP within the information system; and
c. Ensures VoIP equipment used to transmit or discuss sensitive information is protected with agency encryption requirements.

SC-19 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, or when Federal Tax Information is discussed over a Voice over IP telephone system, the agency meets the requirements listed in Section 9.4.15 VoIP Systems of IRS Publication 1075.

SC-20: Secure Name/Address Resolution Service (Authoritative Source)

Agency systems:

a. Provides 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. Provides 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.

SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)

Agency systems requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

SC-22: Architecture and Provisioning for Name/Address Resolution Service

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

SC-23: Session Authenticity

Agency systems protect the authenticity of communications sessions.

SC-28: Protection of Information at Rest

Agency systems protect the confidentiality and integrity of sensitive information at rest regardless of storage media.

SC-28 (enhancement 1): Cryptographic Protection

Agency systems implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information when at rest on system components.

SC-28 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R.§164.312(e)(2)(ii)

SC-28 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the confidentiality and integrity of information at rest shall be protected when located on a secondary (non-mobile) storage device (e.g., disk drive, tape drive) with cryptography mechanisms. Federal Tax Information stored on deployed user workstations, in non-volatile storage, shall be encrypted with FIPS-validated encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology.

The agency does not store Federal Tax Information on Mobile Devices.

SC-39: Process Isolation

The information system maintains a separate execution domain for each executing process.

System & Information Integrity

AIM 216 Minimum Protection Requirement for SI

The Agency will: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

SI-1: System & Information Integrity Policy & Procedures

The agency:

a. Develops, documents, and disseminates to agency leadership & other applicable personnel:
    1. A System & 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 & Information Integrity policy and the associated System & Information Integrity controls;
b. Designates the Chief Information Security Officer to manage the System & Information Integrity policy and procedures;
c. Reviews and updates the current System & Information Integrity:
    1. Policy every three (3) years; and
    2. Procedures annually;
d. Ensures that the System & Information Integrity procedures implement the System & Information Integrity policy and controls; and
e. Develops, documents, and implements remediation actions for violations of the System & Information Integrity policy.

SI-1 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.308(a)(5)(ii)(B); 45 C.F.R.§164.308(a)(6)(ii)

SI-2: Flaw Remediation

The agency:

a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates and corrects other information system flaws (i.e. PoA&M-based flaws) within the following time-periods of the release of updates:
    - For security-relevant software and firmware updates:
        i. Critical – 7 calendar days
        ii. High – 7 calendar days

iii. Moderate/Medium – 15 calendar days
iv. Low – 30 calendar days
v. Informational/Feature addition/enhancement – as tested and approved by agency leadership; and

- For other information systems flaws (i.e. PoA&M-based flaws):
  i. High – 90 calendar days
  ii. Moderate/Medium – 180 calendar days
  iii. Low – 365 calendar days

d. Incorporates flaw remediation into the organizational configuration management process.

SI-2 (enhancement 1): Central Management

The organization centrally manages the flaw remediation process.

SI-2 (enhancement 2): Automated Flaw Remediation Status

The agency employs automated mechanisms weekly to determine the state of system components with regard to flaw remediation.

SI-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(B)

SI-3: Malicious Code Protection

The agency:

a. Implements signature based and non-signature based malicious code protection mechanisms at endpoint and system entry/exit points to detect and eradicate malicious code;
b. Automatically updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
   1. Perform periodic scans of the system weekly and real-time scans of files from external sources at all endpoints and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and
   2. Quarantine malicious code; send alerts to the Administrator, the Security Operations Center, and the CISO; and other organization-defined activities in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

SI-3 (enhancement 1): Central Management

The agency centrally manages malicious code protection mechanisms.

SI-3 (enhancement 2): Automatic Updates

The information system automatically updates malicious code protection mechanisms.

SI-3 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(B); 45 C.F.R. §164.308(a)(6)(ii)

SI-4: Information System Monitoring

The agency:

a. Monitors its systems to detect:
    1. Attacks and indicators of potential of attacks in accordance with organization-defined monitoring objectives; and
    2. Unauthorized local, network, and remote connections;
b. Identify unauthorized use of the system through organization-defined techniques and methods;
c. Invoke internal monitoring capabilities or deploy monitoring devices:
    1. Strategically within the system to collect agency-determined essential information; and
    2. At ad hoc locations within the system to track specific types of transactions of interest to the agency;
d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Adjust the level of system monitoring activity when there is a change in risk to agency operations and assets, individuals, other organizations, or the State;
f. Obtain legal opinion regarding system monitoring activities; and
g. Provide pertinent system monitoring information to system administrators, security operations center personnel, system owners, information owners and other personnel or roles as needed.

SI-4 (enhancement 2): Automated Tools and Mechanisms for Real-time Analysis

The agency employs automated tools and mechanisms to support near real-time analysis of events.

SI-4 (enhancement 4): Inbound and Outbound Communications Traffic

The agency monitors inbound and outbound communications traffic daily during business hours for unusual or unauthorized activities or conditions.

SI-4 (enhancement 5): System Generated Alerts

Agency systems alert the Security Operations Center, system administrators, and other roles and personnel as needed when system-generated indications of compromise or potential compromise occur.

SI-4 (enhancement 7): Automated Response to Suspicious Events

Agency systems notify the Security Operations Center, CISO, system administrators, and other applicable personnel of detected suspicious events and take necessary actions to address suspicious events.

SI-4 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(5)(ii)(B), 45 C.F.R. §164.308(a)(6)(ii)

SI-4 Additional IRS 1075 Requirements

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, agency systems implement host-based monitoring mechanisms.

SI-5: Security Alerts, Advisories, and Directives

The agency:

a. Receives system security alerts, advisories, and directives from multiple external entities on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to agency personnel as needed;
d. Implements security directives in accordance with time frames established by the Information Security Office, or notifies the issuing organization of the degree of noncompliance.

SI-7: Software, Firmware, and Information Integrity

The agency employs integrity verification tools to detect unauthorized changes to software, firmware, and information.

SI-7 (enhancement 1): Integrity checks

Agency systems perform an integrity check of software, firmware, and information daily and at system startup.

SI-7 (enhancement 7): Integration of Detection and Response

Agency systems incorporate the detection of unauthorized security-relevant changes to the system into the organizational incident response capability.

SI-7 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.312(c)(2), 45 C.F.R. §164.312(e)(2)(i), 45 C.F.R. §164.312(c)

SI-8: Spam Protection

The agency:

a. Employs spam protection mechanisms at entry and exit points to detect and act on unsolicited messages; and
b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

SI-8 (enhancement 1): Central Management

The agency centrally manages spam protection mechanisms.

SI-8 (enhancement 2): Automatic Updates

The agency automatically updates spam protection mechanisms.

SI-8 HIPAA mapping

HIPAA: 45 C.F.R.§164.308(a)(5)(ii)(B); 45 C.F.R.§164.308(a)(6)(ii)

SI-10: Information Input Validation

Agency systems check the validity of all information inputs.

SI-11: Error Handling

Agency systems

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 development personnel, system administrators, system owners, and other agency personnel as necessary.

SI-11 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(i)

SI-12: Information Handling and Retention

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

SI-12 HIPAA mapping

45 C.F.R. §164.316(b)(1)(ii); 45 C.F.R. §164.316(b)(2)(i)

SI-16: Memory Protection

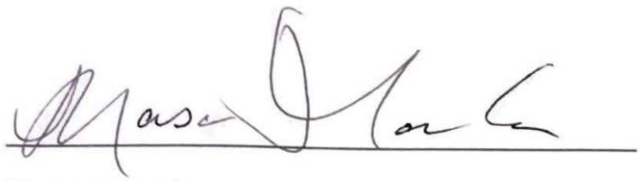
Agency systems implement security safeguards to protect system memory from unauthorized code execution.

Conclusion

Treating information and IT assets as strategic resources allows Medicaid to easily relate business-oriented, risk-based decision processes to this seemingly intangible resource. The creation of clear and precise governance and specific organizational roles with clear responsibilities, both backed by significant support from leadership, will ensure effectiveness of the Security and Privacy Program.

Management Commitment

The undersigned, as the Chief Information Officer of Alabama Medicaid Agency, exercising the power of that office, declares this Security Policy to be available for adoption as of the 30 day of JANUARY, 2020.



Mason L. Tanaka

Alabama Medicaid Agency, Chief Information Officer

Jackie Graham
State Personnel Director
Alice Ann Byrne
Deputy Director

STATE OF ALABAMA

PERSONNEL DEPARTMENT
300 Folsom Administrative Building
Montgomery, Alabama 36130-4100
Telephone: (334) 242-3389 Fax: (334) 242-1110
www.personnel.alabama.gov

MEMORANDUM

TO: Personnel Managers and Payroll Officers

FROM: Jackie Graham
State Personnel Director

DATE: September 3, 2019

SUBJECT: State Holidays for the Year 2020

In order to assist you in planning for the calendar year ahead, we are enclosing a listing of Official State Holidays for 2020. For your convenience, this holiday schedule may also be found on our web site at www.personnel.alabama.gov.

JG/jp

Enclosure

State of Alabama
2020
Official State Holidays

Holiday	Date in 2020
New Year's Day	January 1
Robert E. Lee Martin Luther King, Jr.'s Birthday	January 20
George Washington Thomas Jefferson's Birthday	February 17
Mardi Gras *	February 25
Confederate Memorial Day	April 27
National Memorial Day	May 25
Jefferson Davis' Birthday	June 1
Fourth day of July **	July 4
Labor Day	September 7
Columbus Day Fraternal Day American Indian Heritage Day	October 12
Veterans' Day	November 11
Thanksgiving ***	November 26
Mrs. Rosa L. Parks Day **** (Commemoration Only)	December 1
Christmas Day	December 25

* Mardi Gras is observed only in Baldwin and Mobile Counties. All other State employees are granted one personal leave day each year if in employment status on January 1.

** As the Fourth day of July falls on Saturday, offices will be closed on Friday, July 3, 2020.

*** Upon designation by the Governor.

**** December 1 of each year is designated as Mrs. Rosa L. Parks Day to commemorate her accomplishments. Each resident of Alabama is encouraged to observe the day with suitable activities.