Alabama Medicaid Agency

Information Security Office

Medicaid Enterprise Security Policy – Full Set – Moderate v 1.4

9.14.22

Contents

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 2.2. (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 on 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) & Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)
- 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.

The Organization will:

a. Develop and disseminate an organization-wide information security program plan that:
    1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
    2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
    3. Reflects the coordination among organizational entities responsible for information security; and
    4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
b. Review and update the organization-wide information security program plan annually and following:
    - any significant organizational changes that drive an update to the Agency's Cyber Security strategy;
    - any significant security incidents resulting in the improper disclosure of PII or PHI that meets the notification thresholds identified in applicable Federal and/or State law;
    - the identification of any significant problems with implementing the Information Security Program Plan or Security Controls;

- significant changes to the organization, such that affect the information security office;

c. Protect 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 Organization will appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

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 Organization will:

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;
b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and
c. Make available for expenditure, the planned information security and privacy resources.

PM-4: Plan of Action & Milestones Process

The Organization will:

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

PM-4 HIPAA mapping

45 C.F.R. §164.310(d)

PM-5: System Inventory

The Organization will develop and update, as new systems are instantiated and/or are authorized to operate, an inventory of organizational systems.

PM-6: Measures of Performance

The Organization will develop, monitor, and report on the results of information security and privacy measures of performance.

PM-7: Enterprise Architecture

The Organization will develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

PM-7 HIPAA mapping

45 C.F.R. §164.308(a)(1)(i)

PM-8: Critical Infrastructure Plan

The Organization will address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

PM-9: Risk Management Strategy

The Organization will:

a. Develop a comprehensive strategy to manage:
   1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and
   2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;
b. Implement the risk management strategy consistently across the organization; and
c. Review and update the risk management strategy 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 Organization will:

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

PM-10 HIPAA mapping

45 C.F.R. §164.308(a)(2)

PM-11: Mission & Business Process Definition

The Organization will:

a. Define 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 Nation; and
b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and
c. Review and revise the mission and business processes every three years or as significant changes occur in the organization.

PM-11 HIPAA mapping

45 C.F.R. §164.306(a) and (b)

PM-12: Insider Threat Program

The Organization will implement an insider threat program that includes a cross-discipline insider threat incident handling team.

PM-13: Security and Privacy Workforce

The Organization 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 Organization will:

a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:
    1. Are developed and maintained; and
    2. Continue to be executed; and
b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PM-15: Security and Privacy Groups & Associations

The Organization will:

Establish and institutionalize 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 information, including threats, vulnerabilities, and incidents.

PM-16: Threat Awareness Program

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

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 Organization will:

a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and
b. Review and update the policy and procedures annually.

PM-18: Privacy Program Plan

The Organization will:

a. Develop and disseminate 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 Nation; and
b. Update the plan annually and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.

PM-19: Privacy Program Leadership Role

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: Dissemination of Privacy Program Information

The Organization will:

Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that:

a. Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;
b. Ensures that organizational privacy practices and reports are publicly available; and
c. Employs 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-21: Accounting of DIsclosures

The Organization will:

a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:
    1. Date, nature, and purpose of each disclosure; and
    2. Name and address, or other contact information of the individual or organization to which the disclosure was made;
b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and
c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

PM-22: Personally Identifiable Information Quality Management

The Organization will:

Develop and document organization-wide policies and procedures for:

a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;
b. Correcting or deleting inaccurate or outdated personally identifiable information;
c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and
d. Appeals of adverse decisions on correction or deletion requests.

PM-23: Data Governance Body

The Organization will Establish a Data Governance Body consisting of pertinent organizational roles with related Data Governance responsibilities.

PM-24: Data Integrity Board

The Organization will:

Establish a Data Integrity Board to:

a. Review proposals to conduct or participate in a matching program; and
b. Conduct an annual review of all matching programs in which the agency has participated.

PM-25: Minimization of Personally Identifiable Information used in Testing, Training, and Research

The Organization will:

a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;
b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;

c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and
d. Review and update policies and procedures annually.

PM-26: Compliant Management

The Organization will:

Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and 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;
c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within 90 days;
d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within 30 days; and
e. Response to complaints, concerns, or questions from individuals within 60 days.

PM-27: Privacy Reporting

The Organization will:

a. Develop organizational Privacy Reports and disseminate to:
    1. Applicable oversight entities to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and
    2. Applicable organizational resources and other personnel with responsibility for monitoring privacy program compliance; and
b. Review and update privacy reports annually.

PM-28: Risk Framing

The Organization will:

a. Identify and document:
    1. Assumptions affecting risk assessments, risk responses, and risk monitoring;
    2. Constraints affecting risk assessments, risk responses, and risk monitoring;
    3. Priorities and trade-offs considered by the organization for managing risk; and
    4. Organizational risk tolerance;
b. Distribute the results of risk framing activities to Organizational leadership, Chief Information Officer, Chief Security Officer, and Risk Management Program Leadership Roles; and
c. Review and update risk framing considerations annually.

PM-29: Risk Management Program Leadership Roles

The Organization will:

a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and
b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.

PM-30: Supply Chain Risk Management Strategy

The Organization will:

a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;
b. Implement the supply chain risk management strategy consistently across the organization; and
c. Review and update the supply chain risk management strategy annually or as required, to address organizational changes.

PM-31: Continuous Monitoring Strategy

The Organization will:

Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include:

a. Establishing the following organization-wide metrics to be monitored: per organizational system - # of implemented security controls; # of PoA&M entries(in total and broken down by CRIT/HI/MOD/LOW); estimated mitigation date for highest criticality PoA&M entry (per system);
b. Establishing annual frequencies for monitoring and annual frequencies for assessment of control effectiveness;
c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy;
d. Correlation and analysis of information generated by control assessments and monitoring;
e. Response actions to address results of the analysis of control assessment and monitoring information; and
f. Reporting the security and privacy status of organizational systems to organizational leadership, Chief Information Officer, and Chief Information Security Officer annually.

PM-32: Purposing

The Organization will analyze organizational systems and system components supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.

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 organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:
    1. Organizational and/or System-level access control policy that:
    a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the access control policy and the associated access controls;
b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the access control policy and procedures; and
c. Review and update the current access control:
    1. Policy annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
    2. Procedures annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

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

Organizational systems will:

a. Define and document the types of accounts allowed and specifically prohibited for use within the system (individual, group, system, application, guest/anonymous, emergency, and temporary);
b. Assign account managers;
c. Require organizational Personnel Security requirements, role-based functional need specification, and formal access request from supervisory chain for group and role membership;

d. Specify:
    1. Authorized users of the system;
    2. Group and role membership; and
    3. Access authorizations (i.e., privileges) and other attributes (i.e. account owner information) as required for each account;
e. Require approvals by Agency Commissioner, Deputy Commissioners, Business Owners/Program Manager, Directors, Associate Directors or Supervisors; Human Resources; System Owners (or their designated representative); and/or the Information Security Office for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with organization-defined and/or system-specific procedures, prerequisites, and criteria;
g. Monitor the use of accounts;
h. Notify account managers and designated agency officals within:
    1. 24 hours when accounts are no longer required;
    2. 24 hours when users are terminated or transferred; and
    3. 24 hours when system usage or need-to-know changes for an individual;
i. Authorize access to the system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. Other attributes per the following:
        - as required by the organization or associated missions/business functions;
        - (for systems that receive, process, store or transmit Federal Tax Information) Under the authority to re-disclosed FTI under the provisions of IRC § 6103;
        - (for systems that receive, process, store or transmit Social Security Administration information) possessing need-to-know permission or under the authority to re-disclose SSA data;
j. Review accounts for compliance with account management requirements every 90 days;
k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.

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

Organizational systems support the management of system accounts using agency-managed: ticketing systems; chat/collaboration technologies; email; telephonic; text-messaging; or other automated tools and processes.

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

Organizational systems automatically disable and remove emergency accounts within 24 hours for emergency and two days for temporary accounts.

AC-2 (enhancement 3): Disable Accounts

Organizational systems disable accounts within 24 hours when the accounts:

a. Have expired;

b. Are no longer associated with a user or individual;
c. Are in violation of organizational policy; or
d. Have been inactive for 60 days.

AC-2 (enhancement 4): Automated Audit Actions

Organizational 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 organization requires that users log out or lock their workstation when the user expects to be inactive on their workstation for more than 60 minutes and at the end of their work shift.

AC-2 (enhancement 7): Privileged User Accounts

Organizational Systems will:

a. Establish and administer privileged user accounts in accordance with a role-based access scheme or attribute-based access scheme;
b. Monitor privileged role or attribute assignments;
c. Monitor changes to roles or attributes; and
d. Revoke access when privileged role or attribute assignments are no longer appropriate.

AC-2 (enhancement 9): Restrictions on Use of Shared and Group Accounts

Organizational Systems will not permit the use of shared and group accounts.

AC-2 (enhancement 12): Account Monitoring for Atypical Use

Organizational systems will:

a. Monitor System accounts for atypical usage; and
b. Report atypical usage of system accounts to the Agency Security Operations Center, the owner of the account(s) in question, applicable system owner, and other applicable stakeholders as necessary.

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

The organization disables accounts of individuals within 60 minutes of individuals posing as a significant 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

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

AC-3 (enhancement 7): Role-based Access Control

Organizational systems will enforce a role-based access control policy over defined subjects and objects and control access based upon organization-defined roles and users authorized to assume such roles.

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

Organizational systems enforce approved authorizations for controlling the flow of information within the system and between connected systems based on secure system design, least privilege, need to know, data leakage prevention, technical safeguards and other system-specific information flow control policies in place to protect agency information, Federal Tax Information (where applicable) and to share Social Security Administration data to conduct business (where applicable).

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-5: Separation of Duties

Organizational Systems will:

a. Identify and document organization-defined duties of individuals requiring separation (to prevent malicious activity without collusion); and
b. Define 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

Organizational systems employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

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

The organization will:

Authorize access for users in roles requiring elevated privileges to:

a. The following organization-defined security functions (deployed in hardware, software, and firmware):

    1. Setting/modifying audit logs and auditing behavior;
    2. Setting/modifying boundary protection system rules;
    3. Configuring/modifying access authorizations (i.e., permissions, privileges);
    4. Setting/modifying authentication parameters;
    5. Setting/modifying system configurations and parameters; and
    6. Establishing system accounts; and

b. Security-relevant organizational information (such as Security Incidents, Threat Intelligence, Information relating to Legal Proceedings, etc…).

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

The Organization will Require that users of system accounts (or roles) with access to the following organization-defined security functions (deployed in hardware, software, and firmware): Setting/modifying audit logs and auditing behavior; Setting/modifying boundary protection system rules; Configuring/modifying access authorizations (i.e., permissions, privileges); Setting/modifying authentication parameters; Setting/modifying system configurations and parameters; and Establishing system accounts use non-privileged accounts or roles, when accessing nonsecurity functions.

AC-6 (enhancement 5): PRIVILEGED ACCOUNTS

The organization will restrict privileged accounts on the information system to Security and System admins, personnel or roles requiring privileged access to perform specific activities required by a specific role.

AC-6 (enhancement 6): PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS

Organizational systems prohibit privileged access to the system by non-organizational users.

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

The Organization will:

a. Review quarterly the privileges assigned to privileged roles and roles with access to sensitive information (i.e. FTI or SSA data) to validate the need for such privileges; and
b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

For Systems Containing Federal Tax Information

AC-6 (enhancement 8): PRIVILEGE LEVELS FOR CODE EXECUTION

Organizational systems will prevent the following software from executing at higher privilege levels than users executing the software: all software that does not require elevated privileges for execution.

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

Organizational systems will log the execution of privileged functions.

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

The organization will prevent non-privileged users from executing privileged functions.

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-7: Unsuccessful Logon Attempts

The Organization will:

a. Enforce a limit of 3 consecutive invalid logon attempts by a privileged user and/or 5 consecutive invalid logon attempts by a user during a 120 minute time window; and
b. Automatically lock the account or node for 1 hour or until the lock is released by an administrator when the maximum number of unsuccessful attempts is exceeded and record the event within appropriate security logs when the maximum number of unsuccessful attempts is exceeded.

AC-7 (enhancement 2): PURGE OR WIPE MOBILE DEVICE

Organizational systems will purge or wipe information from smartphones and tablets based on agency Media Sanitization requirements and techniques (if the device supports such capability) after ten (10) consecutive, unsuccessful device logon attempts.

AC-8: System Use Notification

The Organization will:

a. Display the organization's system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
    1. Users are accessing a U.S. Government system;
    2. System usage may be monitored, recorded, and subject to audit;
    3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
    4. Use of the system indicates consent to monitoring and recording;
b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
c. For publicly accessible systems:

1. Display system use information on agency login interfaces for systems and system components that contain sensitive information, before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

The current acceptable message for organizational systems is as follows:

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 Policy PL-4: Rules of Behavior, for additional information.

AC-8 HIPAA mapping

45 C.F.R. §164.520(1)(i)

AC-11: Device Lock

Organizational systems will:

a. Prevent further access to the system by initiating a device lock after fifteen (15) minutes of inactivity (for both remote and internal access connections) or requiring the user to initiate a device lock before leaving the system unattended; and
b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

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

Organizational Systems will conceal, via the device 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

Organizational systems will automatically terminate a user session after 30 minutes of inactivity, and if the interacting user's account becomes locked out for any reason.

AC-14: Permitted Actions without identification or authentication

Organizational Systems will:

a. Identify specific user actions including "attempt login," "shutdown," and any other system-specific user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and
b. Document and provide supporting rationale in the system security plan for the information system, user actions not requiring identification or authentication.

AC-14 HIPAA mapping

45 C.F.R. §164.312(a)(2)(i)

AC-17: Remote Access

Organizational Systems will:

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

AC-17 (enhancement 1): monitoring and control

Organizational systems will employ automated mechanisms to monitor and control remote access methods.

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

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

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

Organizational systems will route remote accesses through authorized and managed network access control points.

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

Organizational systems will:

a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs:
    a. Emergency support for maintaining operations
    b. Support that requires remote access that otherwise would not be able to be performed
    c. Other compelling operational needs; and
b) Document the rationale for remote access in the security plan for the system.

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

Organizational systems will provide the capability to disconnect or disable remote access to the system within 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-18: Wireless Access

Organizational systems will:

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
b. Authorize each type of wireless access to the system prior to allowing such connections.

AC-18 (enhancement 1): AUTHENTICATION AND ENCRYPTION

Organizational systems will protect wireless access to the system using authentication of users and/or devices and encryption.

AC-18 (enhancement 3): DISABLE WIRELESS NETWORKING

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

AC-19: Access Control for Mobile Devices

Organizational systems will:

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

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

Organizational system will employ FIPS 140-validated full-device or container-based encryption to protect the confidentiality and integrity of information on mobile devices containing organizational information or applications (which includes agency-owned and BYOD mobile devices).

AC-20: Use of External Systems

The organization will:

a. Establish defined terms and conditions; and Identify controls asserted to be implemented on external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
    1. Access the system from external systems; and
    2. Process, store, or transmit organization-controlled information using external systems; or
b. Prohibit the use of external systems that are known to be compromised and/or non-Agency-controlled computing and communications devices resident in commercial or public facilities, etc…

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

The Organization will permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

a. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or
b. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

AC-20 (enhancement 2): PORTABLE STORAGE DEVICES – RESTRICTED USE

The Organization will restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using encryption, strictly maintained physical control over portable storage devices, and strict chain of custody documentation.

For Systems Containing Federal Tax Information

AC-20 (enhancement 3): NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE

For Organizational Systems containing Federal Tax Information, the organization restricts the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using Publication 1075 requirements

For Systems Containing Federal Tax Information

AC-20 (enhancement 5): PORTABLE STORAGE DEVICES – PROHIBIT USE

For Organizational Systems containing Federal Tax Information, organizational Systems will prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.

AC-20 HIPAA mapping

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

AC-21: Information Sharing

The Organization will:

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for approved information sharing circumstances where user discretion is required; and
b. Employ automated mechanisms or manual processes to assist users in making information sharing and 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)

For Systems Containing Federal Tax Information

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 Organization will:

a. Designate individuals authorized to make information publicly accessible;
b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information biweekly and remove such information, if discovered.

AC-22 HIPAA mapping

45 C.F.R. §164.502(a)

Additional IRS 1075 Requirements

AC-23: Data Mining Protection

For Organizational Systems containing Federal Tax Information, organizational systems employ agency-defined data mining prevention and detection techniques (including but not limited to: limiting the number and frequency of database queries to increase the work factor needed to determine the contents of databases, limiting types of responses provided to database queries, applying differential privacy techniques or homomorphic encryption, and notifying personnel when atypical database queries or accesses occur) for data storage objects containing Federal Tax Information to detect and protect against unauthorized data mining.

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 organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organizational and/or System-level awareness and training policy that:
    a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

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

b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Awareness and Training policy and procedures; and

c. Review and update the current awareness and training:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

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: Literacy Training and Awareness

The Organization will:

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
    1. As part of initial training for new users and annually thereafter; and
    2. When required by system changes or following any significant security incidents or breaches; following assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;

b. Employ the following techniques to increase the security and privacy awareness of system users:
    - Video-based, Virtualized, or Instructor-led training including but not limited to the following:
        i. Information Security Awareness Training
        ii. HIPAA Privacy and Security Awareness Training
        iii. Social Security Administration Data Security Awareness Training (when applicable):
            1. The sensitivity of SSA data,
            2. The rules of behavior concerning use and security in systems and/or applications processing SSA data,
            3. The Privacy Act and other Federal and state laws governing collection, maintenance, use, and dissemination of information about individuals,
            4. The possible criminal and civil sanctions and penalties for misuse of SSA data (SSA also requires the organization to certify that each employee, contractor, and agent who views SSA data certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure [denoted in TSSR AT-4 control implementation]),
            5. The responsibilities of employees, contractors, and agent's pertaining to the proper use and protection of SSA data,
            6. The restrictions on viewing and/or copying SSA data,
            7. The proper disposal of SSA data,
            8. The security breach and data loss incident reporting procedures,
            9. The basic understanding of procedures to protect the network from viruses, worms, Trojan horses, and other malicious code,
            10. Social engineering (phishing, vishing and pharming) and network fraud prevention.
    - Posters and other printed materials posted around physical office space;
    - Regular mailouts concerning security topics relatable to all levels of employees;
    - Integration of Security Personnel in pertinent meetings/discussions;
    - Phishing emails/campaigns;
    - Other materials, communications, events, etc… as deemed beneficial;
c. Update literacy training and awareness content at least annually and following any significant security incidents or breaches; following assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

Additional IRS 1075 Requirements
AT-2 (enhancement 1): PRACTICAL EXERCISES

The Organization will provide practical exercises in literacy training that simulate events and incidents.

AT-2 (enhancement 2): INSIDER THREAT

The organization will provide literacy training on recognizing and reporting potential indicators of insider threat, 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 (enhancement 3): Social Engineering and Mining

The organization will provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Additional IRS 1075 Requirements
AT-2 (enhancement 4): SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

The Organization will provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using agency security awareness training, periodic mailouts, discussions of such topics in pertinent meetings/gatherings, phishing emails/campaigns; and other materials, communications, events, etc… as deemed beneficial.

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-3: Role-Based Training

The organization will:

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: Privileged Administrators, Developers/Programmers/System Analysts, Security Operation staff, and Supervisors/Managers; (with regards to Federal Tax Information) information system security manager (ISSM); information system security officer (ISSO); personnel having access to FTI:
    1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and
    2. When required by system changes;
b. Update role-based training content at least annually and following any significant security incidents or breaches; following assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

AT-4: Training Records

The organization will:

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
b. Retain individual training records for five years.

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)

AT-6: Training Feedback

The Organization will provide feedback on organizational training results to the following personnel as needed (at least annually): Agency Leadership.

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 organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:
    1. Organizational and/or System-level Audit and Accountability policy that:
        a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
        b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the Audit and Accountability policy and the associated Audit and Accountability controls;
b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Audit and Accountability policy and procedures; and
c. Review and update the current Audit and Accountability:
    1. Policy annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
    2. Procedures annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

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

Organizational Systems will:

a. Identify the types of events that the system is capable of logging in support of the audit function:
    - 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 involving sensitive information;
- Configuration changes;
- Account creation, modification, or deletion;
- Password change;
- File creation, deletion, open, close;
- 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)
- Command-line changes and queries

For systems containing Federal Tax Information, audit the following events in addition to those named in AU-2(a):

1. All accesses or attempts to access an FTI system, including the identity of each user and device;
2. Logoff activities;
3. Activities that might modify, bypass, or negate IT security safeguards;
4. Security-relevant actions associated with processing FTI;
5. User generation of reports and extracts containing FTI;
6. Any interaction with FTI through an application;

For systems containing Social Security Administration Data, audit the following events in addition to those named in AU-2(a):

a. Audit the following events:

i. Viewing SSA data stored within the organization's system;
ii. Viewing of screens that contain SSA data;
iii. All system and data interactions concerning SSA data.

b. Coordinate 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. Determines that the following events are to be audited within the information system:
i. Viewing SSA data stored within the organization's system;
ii. Viewing of screens that contain SSA Data;
iii. All system and data interactions concerning SSA Data;

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system on a continuous basis:
- User log-on and log-off (successful or unsuccessful);
- Configuration changes;
- Application alerts and error messages;
- All system administration activities;
- Modification of privileges and access;
- Account creation, modification, or deletion;
- Concurrent log on from different work stations; and
- Override of access control mechanisms.

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
e. Review and update the event types selected for logging annually, after a significant security incident or breach, or when 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-3: Content of Audit Records

Organizational Systems will ensure that audit records contain information that establishes the following:

a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

AU-3 (enhancement 1): Additional Audit Information

Organizational Systems will generate audit records containing the following additional information (if applicable):

- Filename accessed;
- Program or command used to initiate the event; and

- Source and destination addresses.
- Details that facilitate the reconstruction of events if
    - Unauthorized activity occurs or is suspected; or
    - A malfunction occurs or is suspected

AU-3 (enhancement 3): Limit Personally Identifiable Information Elements

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: username, IP address, hostname, user role (within system).

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-4: Audit Storage Capacity

Organizational systems will allocate audit log storage capacity to accommodate peak log activity and audit record retention requirements.

AU-4 HIPAA mapping

HIPAA: 164.312(b);

AU-5: Response to Audit Processing Failures

Organizational systems will:

a. Alert Systems Administrators and Security Operations Personnel within 15 minutes in the event of an audit logging process failure; and
b. Take the following additional actions:
    1. Attempt to gather logs from alternate sources (i.e. directly from the system components, syslogs servers, etc…) to maintain monitoring capability;
    2. Attempt to overwrite oldest logs with new logs;
    3. Attempt to restore audit logging processes;
    4. If restoration fails, Halt system operations;
    5. If operations halt fails, shut system down until logging processes have been restored (systems that do not support automated shutdown must be shutdown within an hour of audit processing failures).

AU-5 (enhancement 1): STORAGE CAPACITY WARNING

Organizational systems will provide a warning to systems administrators and security operations personnel within 24 hours when allocated audit log storage volume reaches 80% of repository maximum audit log storage capacity.

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

The organization will:

a. Review and analyze system audit records for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity at least per the following schedule:

- Review system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (i.e. malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies within a 24-hour period and on demand and Generate alert notifications for technical personnel review and assessment
- Review network traffic, bandwidth utilization rates, alert notifications, and border defense services to determine anomalies within a 24-hour period and on demand and Generate alerts for technical personnel review and assessment
- Investigate suspicious activity or suspected violations on the Information System and report findings to appropriate officials and take appropriate action
- Use automated utilities to review audit records within a 72-hour period looking for unusual, unexpected, or suspicious behavior
- Inspect Administrator groups on demand and within a 7-day period to ensure unauthorized administrator, system, and privileged application accounts have not been created
- Perform manual reviews of system audit records randomly on demand and within a 30-day period;

b. Report findings to Chief Information Security Officer, Information Security Office/Security Operations Center, Systems Administrators, applicable Supervisors and other applicable roles as necessary; and
c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

AU-6 (enhancement 1): Automated Process Integration

The organization will integrate audit record review, analysis, and reporting processes using automated tools supporting the organization's Security Operations Center.

AU-6 (enhancement 3): Correlate Audit Record Repositories

The organization will analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

AU-6 (enhancement 7): PERMITTED ACTIONS

Specify the permitted actions for each role or user associated with the review, analysis, and reporting of audit record information.

For systems containing Federal Tax Information
AU-6 (enhancement 9): CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES

Correlate information from nontechnical sources with audit record information to enhance 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-7: Audit Reduction & Report Generation

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

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

AU-7 (enhancement 1): Automatic Processing

The Organization will provide and implement the capability to process, sort, and search audit records for events of interest based on the following content:

- Identities of individuals (i.e. user accounts used)
- Event types
- Locations
- Event times
- Event dates
- System resources or components involved in events
- IP addresses involved in events
- Information objects and interactions (i.e. read, write, execute)
- Other content as needed to recognize the likelihood of potential inappropriate access or unauthorized disclosure of sensitive information

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

Organizational Systems will:

a. Use internal system clocks to generate time stamps for audit records; and
b. Record time stamps for audit records that meet accuracy requirements of 100 milliseconds and that use Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), have a fixed local time offset from Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), or that include the local time offset as part of the time stamp.

AU-9: Protection of Audit Information

Organizational systems will:

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
b. Alert System Administrators, Security Operations Personnel, and the pertinent system Information System Security Officers/Managers upon detection of unauthorized access, modification, or deletion of audit information.

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

Organizational Systems will authorize access to management of audit logging functionality to only Security Operations personnel and System Administrators in direct support of Security Operations functions.

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

Organizational systems will retain audit records live in a log repository for at least 90 days and archive for 10 years to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AU-12: Audit Generation

Organizational systems will:

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all possible information system components that receive, process, store, access, protect and/or transmit sensitive information;
b. Allow Information System Security Officers/Managers in conjunction with Systems Administrators and Security Operations Personnel to select the event types that are to be logged by specific components of the system; and
c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

AU-12 (enhancement 1): SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL

Compile audit records from all possible information system components that receive, process, store, access, protect and/or transmit sensitive information into a system-wide (logical or physical) audit trail that is time-correlated to within +/- five (5) minutes for the relationship between time stamps of individual records in the audit trail.

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-organizational Audit Logging

Employ Agency SOC supported or provided log forwarding solutions for coordinating organization-defined audit information among external organizations when audit information is transmitted across organizational boundaries.

For systems containing Federal Tax Information
AU-16 (enhancement 1): Identity Preservation:

Preserve the identity of individuals in cross-organizational audit trails.

For systems containing Federal Tax Information
AU-16 (enhancement 2): Sharing of Audit Information:

Provide cross-organizational audit information to external organizations with which the Agency shares Federal Tax Information based on applicable agency Data Sharing Agreements.

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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level Assessment, Authorization, and Monitoring policy that:
    a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the Assessment, Authorization, and Monitoring policy and the associated Assessment, Authorization, and Monitoring controls;

b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Assessment, Authorization, and Monitoring policy and procedures; and

c. Review and update the current Assessment, Authorization, and Monitoring:

1. Policy annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and

2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

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: Control Assessments

The Organization will:

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;
b. Develop a control assessment plan that describes the scope of the assessment including:
    1. Controls and control enhancements under assessment;
    2. Assessment procedures to be used to determine control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
d. Assess the controls in the system and its environment of operation annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
e. Produce a control assessment report that documents the results of the assessment; and
f. Provide the results of the control assessment to the Authorizing Official (or the AO's Designated Representative), Chief Information Officer, Chief Information Security Officer, Program Manager responsible for the system, and the Information Security Office Governance, Risk, & Compliance Management team within 30 days of its completion.

CA-2 (enhancement 1): Independent Assessors

Employ independent assessors or assessment teams to conduct control assessments.

CA-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(8)

CA-3: Information Exchange

The Organization will:

a. Approve and manage the exchange of information between the system and other systems using interconnection security agreements or other comparable agreements (such as: information exchange security agreements; MoU/MoA; SLA; user agreements; NDA; or specific contractual clause, so long as the appropriate interconnection detail is provided therein);
b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
c. Review and update the agreements annually or whenever significant changes (that can affect the security and privacy state of the system) are implemented that could impact the validity of the agreement as a verification of enforcement of security and privacy requirements.

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 Organization will:

a. Develop a plan of action and milestones for the system to document the planned remediation 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. Update existing plan of action and milestones at least quarterly (or as required based on mitigation timelines) based on the findings from control assessments, independent audits or reviews, 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

Agencies must ensure that the individual and/or office responsible for correcting each weakness is identified in the appropriate POA&M. Agencies must enter all new weaknesses into appropriate POA&Ms within two (2) months for weaknesses identified during assessments.

CA-6: Authorization

The Organization will:

a. Assign a senior official as the authorizing official for the system;
b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;
c. Ensure that the authorizing official for the system, before commencing operations:
    1. Accepts the use of common controls inherited by the system; and
    2. Authorizes the system to operate;
d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
e. Update the authorizations:
    - 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 will develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy 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
    - Vulnerability metrics
b. Establishing a 3 year cycle (1/3 of controls each year and potentially affected controls as part of the Configuration Management Processes) for monitoring and a 3 year cycle (1/3 of controls each year and potentially affected controls as part of the Configuration Management Processes) for assessment of control effectiveness;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of the metrics defined 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 will employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

CA-7 (enhancement 4): Risk Monitoring

The organization will ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

a. Effectiveness monitoring;
b. Compliance monitoring; and
c. Change monitoring.

CA-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 will conduct penetration testing at least annually or when there is a significant change to the system or system components on publicly available systems.

CA-9: Internal System Connections

The Organization will:

a. Authorize internal connections of the following internal information system components or classes of components to the system:
   - Printers, Scanners, & Multi-function devices
   - Communications Equipment
   - Workstations (PC's, Laptops, Notebooks)
   - Servers
   - Hosts within the same zones when applicable
   - Mobile devices (smart phones & tablets);
b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;
c. Terminate internal system connections after the end of the technology's lifecycle, when the information system components or component classes are no longer useful in supporting the organizational mission or applicable business lines, or upon issuance of an order by agency leadership and/or stakeholders; and
d. Review annually the continued need for each internal connection

For systems containing Federal Tax Information
CA-9 (enhancement 1): COMPLIANCE CHECKS

Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.

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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organizational and/or System-level Configuration Management policy that:
    a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the Configuration Management policy and the associated Configuration Management controls;

b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Configuration Management policy and procedures; and

c. Review and update the current Configuration Management:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and

2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

CM-2: Baseline Configuration

Organizational Systems will:

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

b. Review and update the baseline configuration of the system:
    1. Annually;
    2. When required due to reorganization, system architecture or design changes; major system changes/upgrades, critical security patches, and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components); and
    3. When system components are installed or upgraded.

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

Organizational Systems will maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using:

- Hardware and software inventory tools
- Configuration management tools
- Network management tools

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

Organizational systems will retain at least one previous version of baseline configurations of the system to support rollback.

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

Organizational Systems will:

a. Issue dedicated information systems, system components, or devices (laptop, mobile devices) with stringent configurations (FIPS 140-2 encryption, CIS Benchmark Level 1) to individuals traveling to locations that the organization deems to be of significant risk; and
b. Apply the following controls to the systems or components when the individuals return from travel:
    - 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

For systems containing Federal Tax Information
CM-2 (IRS-defined enhancement)

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

CM-3: Configuration Change Control

The Organization will:

a. Determine and document the types of changes to the system that are configuration-controlled;
b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
c. Document configuration change decisions associated with the system;
d. Implement approved configuration-controlled changes to the system;
e. Retain records of configuration-controlled changes to the system for 3 years;
f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through a Change Control Board that convenes monthly, or more frequently to accommodate proposed change requests; when changes:
   - impact Security control implementations
   - impact system architecture/design
   - are more intrusive or impactful than standard support activities (i.e. software patching)

CM-3 (enhancement 2): Testing, Validation, and Documentation of Changes

The Organization will test, validate, and document changes to the system before finalizing the implementation of the changes.

CM-3 (enhancement 4): Security and Privacy Representatives

The Organization will require security and privacy representatives to be members of the change control 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: Impact Analyses

The Organization will analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

CM-4 (enhancement 2): VERIFICATION OF CONTROLS

The Organization will, after system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

CM-5: Access Restrictions for Change

The Organization will define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

CM-5 (enhancement 1): AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS

Organizational Systems will:

a. Enforce access restrictions using automated mechanisms; and

b. Automatically generate audit records of the enforcement actions.

CM-5 (enhancement 5): PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION

a. Limit privileges to change system components and system-related information within a production or operational environment; and

b. Review and reevaluate privileges every 6 months.

For systems containing Federal Tax Information
CM-5 (IRS-defined enhancement)

Restrict administration of configurations to only authorized administrators.

For systems containing Federal Tax Information
CM-5 (IRS-defined enhancement)

Verify the authenticity and integrity of Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI) updates to ensure that the BIOS or UEFI is protected from modification outside of the secure update process.

CM-6: Configuration Settings

Organizational Systems will:

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using Center for Internet Security (CIS) Level 1 Benchmarks or vendor-provided security baselines when available, and other industry standard secure benchmarks/baselines when CIS Benchmarks are not available;
b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for individual components within the information system based on explicitly defined operational requirements; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

CM-6 (enhancement 1): AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION

Manage, apply, and verify configuration settings for system components hosting sensitive information using automated mechanisms.

For systems containing Federal Tax Information
CM-6 (IRS-defined enhancement)

Verify the authenticity and integrity of Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI) updates

CM-7: Least Functionality

Organizational Systems will:

a. Configure the system to provide only essential capabilities; and
b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services:
    - Those not needed to conduct business
    - High-risk or nonsecure (i.e. unencrypted, or non-hardened) functions or capabilities
    - High-risk ports (i.e. 3389, 21/20, 135/137/139/445, etc…)
    - High-risk protocols (i.e. RDP, SMB, FTP, plaintext SMTP, HTTP, etc…)
    - Malicious Software
    - Unsupported software or software that is unable to be hardened
    - (when possible) Hardware or maintenance interfaces that are unused or unnecessary (i.e. PS2, USB, Serial, etc…)
    - For systems containing Federal Tax Information: Those defined in the IRS Office of Safeguards approved compliance requirements (e.g., SCSEMs, assessment tools)

CM-7 (enhancement 1): Periodic review

The Organization will:

a. Review the system monthly to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and
b. Disable or remove high-risk functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

CM-7 (enhancement 2): Prevent Program Execution

Organizational Systems will prevent program execution in accordance with organizational rules authorizing the terms and conditions of software program usage, including but not limited to:

- Software must be legally owned and/or licensed
- Software must be provisioned in approved configurations (i.e. hardened per best practice or approved benchmarks)
- Software must be approved by the organization and documented as authorized
- Users must be authorized for software/application

CM-7 (enhancement 5): Authorized Software – Allow-by-Exception

Organizational Systems will:

a. Identify applications approved and documented as authorized by the organization;
b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and
c. Review and update the list of authorized software programs as new applications or programs are needed to be brought into the environment.

For systems containing Federal Tax Information
CM-7 (enhancement 9): PROHIBITING THE USE OF UNAUTHORIZED HARDWARE

a. Identify agency-defined hardware components authorized for system use;
b. Prohibit the use or connection of unauthorized hardware components;
c. Review and update the list of authorized hardware components annually.

For systems containing Federal Tax Information
CM-7 (IRS-defined enhancement)

Periodically scan FTI networks to detect and remove any unauthorized or unlicensed software.

CM-8: System Component Inventory

Organizational Systems will:

a. Develop and document an inventory of system components that:
    1. Accurately reflects the system;
    2. Includes all components within the system;
    3. Does not include duplicate accounting of components or components assigned to any other system;
    4. Is at the level of granularity deemed necessary for tracking and reporting; and
    5. Includes the following information to achieve system component accountability:

        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. Hardware inventory specifications;
        v. Manufacturer/model information;
        vi. Operating system type and version/service pack level;
        vii. Presence of virtual machines;
        viii. Application software version/license information;
        ix. Physical location (e.g., building/room number);
        x. Logical location (e.g., position with the information system [IS] architecture);
        xi. Media access control (MAC) address;
        xii. IP Address;
        xiii. Component Ownership (for networked components or devices);
        xiv. Operational status;
        xv. Primary and secondary administrators; and
        xvi. Primary user; and

b. Review and update the system component inventory semi-annually.

CM-8 (enhancement 1): Updates During Installation and Removal

Organizational systems will update the inventory of system components as part of component installations, removals, and system updates.

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

Organizational systems will:

a. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms weekly; and
b. Take the following actions when unauthorized components are detected:
    1. Isolate the identified component;
    2. Notify the Security Operations team;
    3. Notify System Administrators;
    4. Notify the responsible individual, and/or individual's Supervisor.

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

Organizational systems will:

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

Organizational systems will develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the system and places the configuration items under configuration management;
d. Is reviewed and approved by Systems Owners, System Administrators, Development teams, Information System Security Managers and/or Officers, other pertinent stakeholders as needed; and
e. Protects the configuration management plan from unauthorized disclosure and modification.

CM-10: Software Usage Restrictions

The Organization will:

a. Use software and associated documentation in accordance with contract agreements and copyright laws;
b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

CM-10 (enhancement 1): Open Source Software

The organization will establish 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 Organization will:

a. Establish the following organization defined policies governing the installation of software by users:
   - Prohibit the installation of software by users on organization-owned and managed client devices (unless approved by the agency CIO, a delegate of the CIO, the agency CISO, or the agency Commissioner)
   - Prohibit the installation of software that has not been reviewed through the organizational software authorization process and documented as Authorized Software;
b. Enforce software installation policies through procedural methods, automated methods, or both; and
c. Monitor policy compliance at least monthly.

CM-12: Information Location

Organizational Systems will:

a. Identify and document the location of PII, PHI, and any other Federally-regulated information and the specific system components on which the information is processed and stored;
b. Identify and document the users who have access to the system and system components where the information is processed and stored; and
c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

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

Organizational Systems will use automated tools to identify PII, PHI, and any other Federally-regulated information on organizational system components to ensure controls are in place to protect organizational information and individual privacy.

For systems containing Federal Tax Information
CM-13: Data Action Mapping

The organization will Develop and document a map of system data actions.

For systems containing Federal Tax Information
CM-14: Signed Components

Prevent the installation of software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and System-level Contingency Planning policy that:
    a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the Contingency Planning policy and the associated Contingency Planning controls;

b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Contingency Planning policy and procedures; and

c. Review and update the current Contingency Planning:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

CP-1 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(7)(i)

CP-2: Contingency Plan

Organizational Systems will:

a. Develop a contingency plan for the system that:
    1. Identifies essential mission and business functions and associated contingency requirements;
    2. Provides recovery objectives, restoration priorities, and metrics;
    3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
    4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
    5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;

6. Addresses the sharing of contingency information; and
7. Is reviewed and approved by System Owner or Program Manager or other Organizational Leadership;

b. Distribute copies of the contingency plan to the Information Security Office, Program Manager, Business Owner, personnel coordinating the Contingency Plan, and other stakeholders identified within the contingency plan;
c. Coordinate contingency planning activities with incident handling activities;
d. Review the contingency plan for the system annually;
e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicate contingency plan changes to Information Security Office, Program Manager, Business Owner, personnel coordinating the Contingency Plan, and other stakeholders identified within the contingency plan;
g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
h. Protect the contingency plan from unauthorized disclosure and modification.

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

Organizational Systems will coordinate contingency plan development with organizational elements responsible for related plans.

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

Organizational Systems will plan for the resumption of essential mission and business functions within the Maximum Tolerable Downtime for the system or within 72 hours of contingency plan activation.

CP-2 (enhancement 8): Identify critical assets

Organizational systems will identify critical system assets supporting essential mission and 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

Organizational Systems will:

a. Provide contingency training to system users consistent with assigned roles and responsibilities:
   1. Within 30 days of assuming a contingency role or responsibility;
   2. When required by system changes; and
   3. Annually thereafter; and
b. Review and update contingency training content every three years and following significant changes to the Contingency Plan and/or System/Environment.

CP-3 HIPAA mapping

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

CP-4: Contingency Plan Testing

Organizational Systems will:

a. Test the contingency plan for the system annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan:
   - Tests developed from NIST 800-34 guidelines
   - Tests developed from NIST 800-84 guidelines (where applicable);
b. Review the contingency plan test results; and
c. Initiate corrective actions, if needed.

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

Organizational Systems will coordinate contingency plan testing with organizational elements responsible for related plans.

CP-6: Alternate Storage Site

Organizational Systems will:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and
b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

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

Organizational Systems will identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

CP-6 (enhancement 3): Accessibility

Organizational Systems will identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline 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-7: Alternate Processing Site

Organizational Systems will:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of system operations for essential mission and business functions within 72

hours, or within the Maximum Tolerable Downtime for the system when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and
c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

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

Organizational Systems will identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

CP-7 (enhancement 2): Accessibility

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-7 (enhancement 3): Priority of Service

Organizational Systems will develop alternate processing site agreements that contain priority-of-service provisions in accordance with 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-8: Telecommunication Services

Organizational Systems will establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within 72 hours, or within the Maximum Tolerable Downtime for the system 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

Organizational Systems will:

a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and
b. 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

Organizational Systems will obtain 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

Organizational Systems will:

a. Conduct backups of user-level information contained in the system – weekly full & daily incremental/differential or according to the Recovery Point Objective defined in the related Contingency Plan, whichever is shorter;
b. Conduct backups of system-level information contained in the system – weekly full & daily incremental/differential or according to the Recovery Point Objective defined in the related Contingency Plan, whichever is shorter;
c. Conduct backups of system documentation, including security- and privacy-related documentation – weekly full; and
d. Protect the confidentiality, integrity, and availability of backup information.

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

Organizational Systems will Test backup information at least every 6 months to verify media reliability and information integrity.

CP-9 (enhancement 8): Cryptographic protection

Organizational Systems will Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of system backup information.

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-10: System Recovery and Reconstitution

Organizational Systems will Provide for the recovery and reconstitution of the system to a known state within the time frames specified in the associated Contingency Plan after a disruption, compromise, or failure.

CP-10 (enhancement 2): Transaction Recovery

Organizational Systems will implement 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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and System-level Identification and Authentication policy that:
    a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the Identification and Authentication policy and the associated Identification and Authentication controls;

b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Identification and Authentication policy and procedures; and

c. Review and update the current Identification and Authentication:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

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)

Organizational Systems will uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

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

Organizational Systems will implement multi-factor authentication for access to privileged accounts.

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

Organizational Systems will implement multi-factor authentication for access to non-privileged accounts.

For systems containing Federal Tax Information
IA-2 (enhancement 6): Access to Accounts – Separate Device:

Organizational Systems implement multi-factor authentication for remote access to privileged accounts and non-privileged accounts such that:

a. One of the factors is provided by a device separate from the system gaining access; and

b. The device meets Authenticator Assurance Level 2 (AAL) per NIST SP 800-63.

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

Organizational Systems will Implement replay-resistant authentication mechanisms for access to privileged accounts and non-privileged accounts.

IA-2 (enhancement 12): Acceptance of PIV credentials

Organizational systems will Accept and electronically verify Personal Identity Verification-compliant credentials – when available.

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-3: Device Identification & Authentication

Organizational systems will uniquely identify and authenticate servers (physical or virtual), workstations (physical or virtual, PC's/Desktops or laptops), and other devices defined in the applicable SSP before establishing a local, remote, or network connection.

For systems containing Federal Tax Information
IA-3 (enhancement 1): CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION

Authenticate all devices before establishing a remote network connection using bidirectional authentication that is cryptographically based.

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

Organizational Systems will manage system identifiers by:

a. Receiving authorization from System Administrators and the Supervisory Chain to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;
c. Assigning the identifier to the intended individual, group, role, service, or device; and
d. Preventing reuse of identifiers indefinitely.

IA-4 (enhancement 4): Identify User Status

Organizational Systems will Manage individual identifiers by uniquely identifying each individual as:

- Employee
- Non-Employee/Contractor
- **For systems containing Federal Tax Information -** Change all default vendor-set or factory-set administrator accounts prior to implementation (e.g., during installation or immediately after installation)

IA-4 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

Organizational systems will manage 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. Changing/refreshing authenticators as follows:
    - 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; 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 (when available);
    - 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.
g. Protecting authenticator content from unauthorized disclosure and modification;
h. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

i. Changing authenticators for group/role accounts when membership to those accounts changes.

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

For password-based authentication, organizational systems will:

a) Maintain a list of commonly-used, expected, or compromised passwords and update the list at least annually and when organizational passwords are suspected to have been compromised directly or indirectly;
b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
c) Transmit passwords only over cryptographically-protected channels;
d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
e) Require immediate selection of a new password upon account recovery;
f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
g) Employ automated tools to assist the user in selecting strong password authenticators; and
h) Enforce the following composition and complexity rules:
    a. At least 8 characters in length for non-privileged accounts, and at least 15 characters in length for privileged accounts (including accounts with access to Federal Tax Information);
    b. Use at least one character from each of the four character categories (A-Z, a-z, 0-9, special characters);
    c. Enforces at least a minimum of six (6) characters change when new passwords are created;
    d. Prevents password reuse for 24 generations;
    e. Allows the use of a temporary password for system logons with an immediate change to a permanent password;
    f. Employs automated tools to assist the user in selecting strong password authenticators (when applicable);
    g. Prohibits the use of dictionary names or words.

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

a. For public key-based authentication, organizational systems will:
    1. Enforce authorized access to the corresponding private key; and
    2. Map the authenticated identity to the account of the individual or group; and
b. When public key infrastructure (PKI) is used, organizational systems will:
    1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
    2. Implement a local cache of revocation data to support path discovery and validation.

For systems containing Federal Tax Information
IA-5 (enhancement 5): CHANGE AUTHENTICATORS PRIOR TO DELIVERY

Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.

IA-5 (enhancement 6): Protection of Authenticators

Organizational Systems will protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

For systems containing Federal Tax Information
IA-5 (enhancement 7): NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

For systems containing Federal Tax Information
IA-5 (enhancement 12): BIOMETRIC AUTHENTICATION PERFORMANCE

For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements: as defined in NIST SP 800-63.

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

Organizational systems will obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and 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

Organizational systems will 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)

Organizational systems will uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

IA-8 (enhancement 2): Acceptance of External Authenticators

When applicable, Organizational systems will:

a. Accept only external authenticators that are NIST-compliant; and
b. Document and maintain a list of accepted external authenticators.

IA-8 (enhancement 4): Use of Defined Profiles

When applicable, Organizational systems will conform to the following profiles for identity management: NIST or FICAM authentication protocols such as SAML and OpenID.

IA-8 HIPAA mapping

45 C.F.R. §164.312(a)(2)(i)

For systems containing Federal Tax Information

IA-9: SERVICE IDENTIFICATION AND AUTHENTICATION

Uniquely identify and authenticate web applications using digital certificates or services or applications that query a database before establishing communications with devices, users, or other services or applications.

IA-11: Re-Authentication

Organizational systems will require users to re-authenticate:

- When devices are unlocked
- When roles, authenticators, or credentials change (i.e. switching to privileged user role from a non-privileged user role)
- When the execution of privileged functions occur
- After extended periods of time

IA-12: Identity Proofing

Organizational systems will:

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;
b. Resolve user identities to a unique individual; and
c. Collect, validate, and verify identity evidence.

IA-12 (enhancement 1): SUPERVISOR AUTHORIZATION

Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

IA-12 (enhancement 2): Identity Evidence

Organizational systems will require evidence of individual identification be presented to the registration authority.

IA-12 (enhancement 3): Identity Evidence Validation and Verification

Organizational systems will require that the presented identity evidence be validated and verified through NIST SP 800-63 compliant methods of validation and verification.

IA-12 (enhancement 5): Address Confirmation

Organizational systems will Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record

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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and/or System-level Incident Response policy that:
    a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the Incident Response policy and the associated Incident Response controls;

b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Incident Response policy and procedures; and

c. Review and update the current Incident Response:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

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 Organization will:

a. Provide incident response training to system users consistent with assigned roles and responsibilities:
    1. Within 30 days of assuming an incident response role or responsibility or acquiring system access;
    2. When required by system changes; and
    3. annually thereafter; and

b. Review and update incident response training content at least Annually and following significant security incidents and system changes.

For systems containing Federal Tax Information
IR-2 (enhancement 1): SIMULATED EVENTS

Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

For systems containing Federal Tax Information
IR-2 (enhancement 3): BREACH

Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

IR-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(6)(i)

IR-3: Incident Response Testing

The Organization will test the effectiveness of the incident response capability for the system annually using the following tests: 1) Checklists; 2) Walk-throughs; 3) TableTop exercises; or 4) Simulations (parallel or full interrupt) to determine the incident response effectiveness, and document the results.

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

The Organization will Coordinate incident response testing with organizational elements responsible for related plans.

For systems containing Federal Tax Information
IR-3 (enhancement 3): CONTINUOUS IMPROVEMENT

Use qualitative and quantitative data from testing to:

a. Determine the effectiveness of incident response processes;
b. Continuously improve incident response processes; and
c. Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

IR-3 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(6)(i)

IR-4: Incident Handling

The Organization will:

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinate incident handling activities with contingency planning activities;
c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and
d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

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

The Organization will support the incident handling process using automated tools that support event log correlation, endpoint protection/detection & response, remote forensics, and other applicable tools.

For systems containing Federal Tax Information
IR-4 (enhancement 6): INSIDER THREATS

Implement an incident handling capability for incidents involving insider threats.

For systems containing Federal Tax Information
IR-4 (enhancement 8): CORRELATION WITH EXTERNAL ORGANIZATIONS

Coordinate with contractors, datacenters, counties, and other agencies to correlate and share incidents involving FTI to achieve a cross-organization perspective on incident awareness and more effective incident responses.

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 will track and document 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 Organization will:

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

IR-6 (enhancement 1): Automated Reporting

The Organization will report incidents using emails, incident tracking/ticketing systems, collaboration tools, and other automated incident response tools and applications as needed.

For systems containing Federal Tax Information
IR-6 (enhancement 2): VULNERABILITIES RELATED TO INCIDENTS

Report system vulnerabilities associated with reported incidents to agency helpdesk and/or Security Operations Center and the Privacy Office and related Federal partners.

IR-6 (enhancement 3): Supply Chain Coordination

The Organization will provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident

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-7: Incident Response Assistance

The Organization will provide an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the system for the handling and reporting of incidents.

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

The Organization will increase the availability of incident response information and support using communications tools such as email and other collaborative platforms; threat intelligence feeds and platforms; and other tools in support of incident response assistance.

IR-7 (enhancement 2): COORDINATION WITH EXTERNAL PROVIDERS

a. Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and
b. Identify organizational incident response team members to the external providers.

IR-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. Addresses the sharing of incident information;
9. Is reviewed and approved by the Chief Information Officer Annually; and
10. 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, and where applicable, Agency Personnel Resources with access to Federal Tax Information;
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 and where applicable, Agency Personnel Resources with access to Federal Tax Information,
e. Protects the Incident Response plan from unauthorized disclosure and modification.

For systems containing Federal Tax Information
IR-8 (enhancement 1): BREACHES

The Organization will include the following in the Incident Response Plan for breaches involving personally identifiable information:

a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
c. Identification of applicable privacy requirements.

IR-8 HIPAA mapping

45 C.F.R. §164.308(a)(6) C.F.R

IR-9: Information Spillage Response

The Organization will Respond to information spills by:

a. Assigning Agency Security Operations Center staff and other support personnel as needed with responsibility for responding to information spills
b. Identifying the specific information involved in the information system contamination
c. Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill
d. Isolating the contaminated information system or system component
e. Eradicating the information from the contaminated information system or component
f. Identifying other information systems or system components that may have been subsequently contaminated
g. Performing the following additional actions: additional actions necessary to isolate, communicate (information about information spillage to Agency leadership, system owners, and data owners/custodians), remediate spillage, and notify affected individuals as well as Federal and State Authorities as required by State and Federal Law.

IR-9 (enhancement 2): TRAINING

Provide information spillage response training Annually.

IR-9 (enhancement 3): POST-SPILL OPERATIONS

Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: 1) Contain the spillage by identifying all hardware, software systems, and applications affected; 2) Sanitize using approved mechanisms to permanently remove the data spilled from contaminated information systems, applications, and media; and 3) If sanitization is not affective, then replace or reimage applications and media.

IR-9 (enhancement 4): EXPOSURE TO UNAUTHORIZED PERSONNEL

Employ the following controls for personnel exposed to information not within assigned access authorizations:

1. Remind individuals of
    a. PL-4: Rules of Behavior;
    b. PS-6: Access Agreements (including Non-Disclosure Agreements);
2. Review Accesses associated with individuals' credentials
3. Remove unnecessary accesses
4. Follow PS-8: Personnel Sanctions practices if necessary

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: System Maintenance Policy & Procedures

The Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

3. Organization-level and/or System-level System Maintenance that:

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

d) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

4. Procedures to facilitate the implementation of the System Maintenance policy and the associated System Maintenance controls;

b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the System Maintenance policy and procedures; and

c. Review and update the current System Maintenance:

3. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and

4. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

MA-2: Controlled Maintenance

The Organization:

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c. Require that the applicable System Owner, or other applicable official explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: all information;

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in organizational maintenance records:
    - Date & time of maintenance
    - Name of individuals or group performing maintenance
    - Name of escort, if applicable
    - Description of maintenance performed
    - System components removed or replace – including asset/inventory information

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 will:

a. Approve, control, and monitor the use of system maintenance tools; and
b. Review previously approved system maintenance tools every 30 days.

MA-3 (enhancement 1): Inspect Tools

The Organization will inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

MA-3 (enhancement 2): Inspect Media

The Organization will check media containing diagnostic and test programs for malicious code before the media are used in the system.

MA-3 (enhancement 3): Prevent Unauthorized Removal

The Organization 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.

For systems containing Federal Tax Information
MA-3 (enhancement 4): RESTRICTED TOOL USE

Restrict the use of maintenance tools to authorized personnel only.

For systems containing Federal Tax Information
MA-3 (enhancement 5): EXECUTION WITH PRIVILEGE

Monitor the use of maintenance tools that execute with increased privilege.

MA-4: Nonlocal Maintenance

The Organization will:

a. Approve and monitor nonlocal maintenance and diagnostic activities;
b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintain records for nonlocal maintenance and diagnostic activities; and
e. Terminate session and network connections when nonlocal maintenance is completed.

1 & 2, 3 & 5

MA-4 (enhancement 1): LOGGING AND REVIEW

a. Log organizational system components for nonlocal maintenance and diagnostic sessions; and
b. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

MA-4 (enhancement 3): COMPARABLE SECURITY AND SANITIZATION

a. Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or
b. Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

For systems containing Federal Tax Information
MA-4 (enhancement 4): AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS

Protect nonlocal maintenance sessions by:

a. Employing replay-resistant authenticators; and
b. Separating the maintenance sessions from other network sessions with the system by either:
    1. Physically separated communications paths; or
    2. Logically separated communications paths.

MA-4 (enhancement 5): APPROVALS AND NOTIFICATIONS

a. Require the approval of each nonlocal maintenance session by personnel with sufficient information security and system knowledge to determine the appropriateness of the proposed maintenance; and

b. Notify the following personnel or roles of the date and time of planned nonlocal maintenance: System Owners and other applicable stakeholders.

For systems containing Federal Tax Information
MA-4 (enhancement 6): CRYPTOGRAPHIC PROTECTION

Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: Cryptographic protection requirements as specified in SC-13: Cryptographic Protections.

For systems containing Federal Tax Information
MA-4 (enhancement 7): DISCONNECT VERIFICATION

Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

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-5: Maintenance Personnel

The Organization will :

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

MA-5 (enhancement 1): INDIVIDUALS WITHOUT APPROPRIATE ACCESS

a. Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
    1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities;
    2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components.
b. Develop and implement mitigating controls in the event a system component cannot be sanitized, removed, or disconnected from the system.

MA-5 (enhancement 4): FOREIGN NATIONALS

Ensure that:

a. Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and
b. Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements.

MA-5 (enhancement 5): NON-SYSTEM MAINTENANCE

Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.

MA-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 will obtain maintenance support and/or spare parts for production system components within the applicable Recovery Time Objective (RTO) specified in the contingency plan.

MA-6 (enhancement 1): PREVENTIVE MAINTENANCE

Perform preventive maintenance on critical system components at the applicable Recovery Time Objective (RTO) specified in the contingency plan.

MA-6 (enhancement 2): PREDICTIVE MAINTENANCE

Perform predictive maintenance on critical system components at the applicable Recovery Time Objective (RTO) specified in the contingency plan.

MA-6 (enhancement 3): AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE

Transfer predictive maintenance data to a maintenance management system using automated mechanisms.

MA-6 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(a)(2)(iv)

MA-7: Field Maintenance

Restrict or prohibit field maintenance on system components to trusted maintenance facilities.

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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and/or System-level Media Protection that:
    e) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    f) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the Media Protection policy and the associated Media Protection controls;

b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Media Protection policy and procedures; and

c. Review and update the current Media Protection:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and

2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

MP-2: Media Access

The agency restricts access to sensitive digital and non-digital media (media containing sensitive information) 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 media or hardware components (whether or not it contains sensitive information) from marking if the media remains within a strictly agency-controlled environment.

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.

For systems containing Federal Tax Information

Reference Section 2.B, Secure Storage - IRC § 6103(p)(4)(B), on additional secure storage requirements

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-5: Media Transport

The agency:

a. Protects and controls digital and non-digital media containing sensitive information during transport outside of controlled areas using FIPS 140-2 and/or SC-28: Protection of Information at Rest compliant 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.

For systems containing Federal Tax Information
MP-5 (enhancement 3): CUSTODIANS

Employ an identified custodian during transport of system media outside of controlled areas.

MP-5 HIPAA mapping

45 C.F.R. §164.312(a)(2)(iv)

MP-6: Media Sanitization

The Organization will:

a. Sanitize digital and non-digital media containing sensitive information or organizational intellectual property prior to disposal, release out of organizational control, or release for reuse using purge, destroy, or cryptographic sanitization techniques and procedures per the latest revision of NIST 800-88 and in accordance with applicable federal and organizational standards and policies; and
b. Employ sanitization mechanisms 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 (enhancement 2): EQUIPMENT TESTING

Test sanitization equipment and procedures annually to ensure that the intended sanitization is being achieved.

For systems containing Federal Tax Information

(IRS-Defined): Clear or purge any sensitive data from the system BIOS or UEFI before a computer system is disposed of and leaves the agency. Reset the BIOS or UEFI to the manufacturer's default profile, to ensure the removal of sensitive settings such as passwords or keys.

(IRS-Defined): Media provided by foreign visitors (end users) may only be loaded into a standalone agency system. The system must remain standalone until such time as it is sanitized. Additionally, no other media loaded into the standalone system can be loaded into a non-standalone agency system until sanitized.

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-7: Media Use

The Organization will:

a. Prohibit the use of media not controlled by the organization (such as flash drives, external hard disk drives, and other portable storage devices) on organizational systems or system components using organizational media review techniques and processes; and
b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Control Enhancements:

For systems containing Federal Tax Information

(IRS-Defined): Develop policy to disable all portable storage devices with the exception of those required for explicit business need, which shall be restricted to specific workstations or laptops. In the absence of an agency-developed and issued policy, the default policy is:

a. That the connection of non-agency portable storage devices is disallowed; and

b. Technical controls are implemented to enforce the policy (e.g., Implement data loss prevention software to limit the use of removable media to known devices, blacklist usb-storage, prevent the mounting of USB storage, Deny All Access to All Removable Storage Classes).

For systems connecting to the CMS Hub
MP-CMS-1: Media Related Records

Inventory and disposition records for information system media shall be maintained to ensure control and accountability of sensitive information. The media-related records shall contain sufficient information to reconstruct the data in the event of a breach.

Implementation Standards

1. The media records must, at a minimum, contain:
a. The name of media recipient;
a. Signature of media recipient;
b. Date/time media received;
c. Media control number and contents;
d. Movement or routing information; and
e. If disposed of, the date, time, and method of destruction.

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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and/or System-level Physical & Environmental Protection 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. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Physical & Environmental Protection policy and procedures; and

c. Review and update the current Physical & Environmental Protection:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

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 Organization will:

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;
b. Issue authorization credentials for facility access;
c. Review the access list detailing authorized facility access by individuals within every 180 days; and
d. Remove individuals from the facility access list when access is no longer required.

PE-2 (enhancement 1): Access by Position or Role

Authorize physical access to the facility where the system resides based on position or role.

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-3: Physical Access Control

The Organization will:

a. Enforce physical access authorizations (as permitted by fire and safety requirements) at entry and exit points to the facility where the system resides by:
    1. Verifying individual access authorizations before granting access to the facility; and
    2. Controlling ingress and egress to the facility using keys, locks, combinations, biometric readers, card readers, and/or guards;
b. Maintain physical access audit logs for applicable entry or exit points;
c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: keys, locks, combinations, biometric readers, card readers, and/or guards;
d. Escort visitors and control visitor activity while inside areas not officially designated as publicly accessible (i.e. access controlled areas);
e. Secure keys, combinations, and other physical access devices;
f. Inventory physical access devices, such as keys, badges/cards, card readers, and locks annually; and
g. Change combinations at least annually and keys annually and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

For systems containing Federal Tax Information

PE-3 (enhancement 2): Facility and Systems

Perform security checks at a minimum daily at the physical perimeter of the facility or system for exfiltration of information or removal of system components.

PE-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 Organization will Control physical access to communications closets and information system distribution and transmission lines within organizational facilities using physical/key locks, cameras, locking equipment racks, and/or other applicable physical security mechanisms.

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 organization will control physical access to output from organizational devices displaying sensitive information or organizational intellectual property 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 Organization will:

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;
b. Review physical access logs at least weekly and upon occurrence of security incidents or indications of potential events involving physical security; and
c. Coordinate results of reviews and investigations with the organizational incident response capability.

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

The Organization will monitor physical access to the facility where the system resides using 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 Organization will:

a. Maintain visitor access records to the facility where the system resides for at least 5 years;
b. Review visitor access records (that include: 1. Name and organization of the person visiting; 2. Visitor's Signature; 3. Form of Identification; 4. Date of access; 5. Time of entry and departure; 6.

Purpose and level of access for visit; 7. Name and organization of person visited) at least monthly; and

c. Report anomalies in visitor access records to Physical Security Team, the Security Operations Center (if physical security events align with logical security events), and organizational leadership.

PE-9: Power Equipment and Cabling

The Organization will protect power equipment and power cabling for the system from damage and destruction.

PE-10: Emergency Shutoff

The Organization will:

a. Provide the capability of shutting off power to information systems or individual system components in emergency situations;
b. Place emergency shutoff switches or devices in a location that does not require personnel to approach equipment to facilitate access for authorized personnel; and
c. Protect emergency power shutoff capability from unauthorized activation.

PE-11: Emergency Power

The Organization will Provide an uninterruptible power supply to facilitate an orderly shutdown of the system or transition of the system to long-term alternate power in the event of a primary power source loss.

PE-12: Emergency Lighting

The Organization will employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

PE-13: Fire Protection

The Organization will employ and maintain fire detection and suppression systems that are supported by an independent energy source.

PE-13 (enhancement 1): Automatic Fire Detection

The Organization will Employ fire detection systems that activate automatically and notify Physical Security Team, Data Center Management Team and local emergency responders in the event of a fire.

PE-14: Temperature and Humidity Controls

The Organization will:

a. Maintain temperature and humidity levels within the facility where the system resides within acceptable vendor-specified levels; and
b. Monitor environmental control levels at least daily.

PE-15: Water Damage Protection

The Organization will Protect the 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 Organization will:

a. Authorize and control all information system components entering and exiting the facility; and
b. Maintain records of the system components.

PE-17: Alternate Work Site

The Organization will:

a. Determine and document the organizational alternate work sites allowed for use by employees;
b. Employ the following controls at alternate work sites: all security controls applicable to the primary site;
c. Assess the effectiveness of controls at alternate work sites; and
d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

PE-17 HIPAA mapping

HIPAA: 45 C.F.R. §164.310(a)(2)(i)

For systems containing Federal Tax Information

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 2.B.7 in IRS Publication 1075 Telework Locations for off-site locations such as other government facilities or private residences of employees.

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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and/or System-level Planning that:
    a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

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

b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Planning policy and procedures; and

c. Review and update the current Planning:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

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

Organizational Systems will:

a. Develop security and privacy plans for the system that:
    1. Are consistent with the organization's enterprise architecture;
    2. Explicitly define the constituent system components;
    3. Describe the operational context of the system in terms of mission and business processes;
    4. Identify the individuals that fulfill system roles and responsibilities;
    5. Identify the information types processed, stored, and transmitted by the system;
    6. Provide the security categorization of the system, including supporting rationale;
    7. Describe any specific threats to the system that are of concern to the organization;

8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
10. Provide an overview of the security and privacy requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
13. Include risk determinations for security and privacy architecture and design decisions;
14. Include security- and privacy-related activities affecting the system that require planning and coordination with the organizational security team, the organizational privacy team (if applicable), and any other applicable resource; and
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to Information Owner, System Owner, Chief Information Officer, Chief Information Security Officer, and other applicable personnel or roles;
c. Review the plans at least annually;
d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
e. Protect the plans from unauthorized disclosure and modification

For systems containing Federal Tax Information

(IRS-Defined): Include or reference a plan for media sanitization and disposition that addresses all system media and backups in the agency's system security and privacy plans

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-4: Rules of Behavior

The Organization will:

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;
b. Receive a documented 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 system;
c. Review and update the rules of behavior at least annually; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated.

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

The Organization will Include in the rules of behavior, restrictions on:

a. Use of social media, social networking sites, and external sites/applications;
b. Posting organizational information on public websites; and
c. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

For systems containing Federal Tax Information

(IRS-Defined): Unless superseded by centrally-issued cross-agency policy, establish usage restrictions and implementation guidance for using Internet-supported technologies (e.g. Instant messaging) based on the potential for these technologies to cause damage or disruption to the information system or the agency's accomplishment of its mission. Document the use of Internet-supporting technologies

PL-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

Organizational Systems will:

a. Develop security and privacy architectures for the system that:
    1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
    2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
    3. Describe how the architectures are integrated into and support the enterprise architecture; and
    4. Describe any assumptions about, and dependencies on, external systems and services;
b. Review and update the architectures at least every three years to reflect changes in the enterprise architecture; and
c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

For systems containing Federal Tax Information

IRS - CE-1) Defense-In-Depth: Design the security and privacy architectures for the system using a defensein-depth approach that: a. Allocates system communication and other relevant controls to information systems processing, storing, and transmitting FTI; and b. Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner

PL-10: Baseline Selection

Organizational Systems will Select a control baseline for the system.

PL-11: Baseline Tailoring

Organizational Systems will Tailor 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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and/or System-level Personnel Security Policy & Procedures that:
    a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the Personnel Security policy and the associated Personnel Security controls;

b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Personnel Security policy and procedures; and

c. Review and update the current Personnel Security:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and

2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

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 Organization will:

a. Assign a risk designation to all organizational positions;
b. Establish screening criteria for individuals filling those positions; and
c. Review and update position risk designations at least every 3 years 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 system and/or sensitive information;
b. Rescreens individuals at least every 5 years and anytime the individual moves to a new position with a higher risk designation.

For systems containing Federal Tax Information

With respect to agency systems that receive, process, store, transmit, or dispose of Federal Tax Information, the agency meets the requirements listed in Section 2.C.3 Background Investigation Minimum Requirements of IRS Publication 1075.

PS-4: Personnel Termination

The Organization will, upon termination of individual employment:

a. Disable system access within the process of termination, if possible, if not, at least within 24 hours; and notify individual's chain of command, Human Resources, Helpdesk, the Information Security Office, and other applicable personnel and roles of the termination;
b. Terminate or revoke any authenticators and credentials associated with the individual;
c. Conduct exit interviews that include a discussion of exit reasoning, reminder of agreed upon Rules of Behavior, non-disclosure of sensitive information (including Intellectual Property), information security, and any related privacy information; and if applicable, immediately escorts employees terminated for cause out of the organization;
d. Retrieve all security-related organizational system-related property; and
e. Retain access to organizational information and systems formerly controlled by terminated individual.

PS-5: Personnel Transfer

The Organization will:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiate the following transfer or reassignment actions as soon as possible but no later than 30 days:
    1. Re-issuing or confirming the need to continue to have/access appropriate information system-related property (e.g., keys, identification cards, building passes);
    2. Notifying security management;
    3. Closing obsolete accounts and establishing new accounts; and
    4. When an employee moves to a new position of trust, re-evaluating logical and physical access controls;
c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify the individual's chain of command, Human Resources, Helpdesk, the Security team, and other applicable personnel and roles within 5 business days.

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 Organization will:

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

For systems containing Federal Tax Information

PS-6: Access Agreements (enhancement 3): Post-Employment Requirements

The Organization will:

a. Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and
b. Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information

PS-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 Organization will:

a. Establish personnel security requirements, including security roles and responsibilities for external providers;
b. Require external providers to comply with personnel security policies and procedures established by the organization;
c. Document personnel security requirements;

d. Require external providers to notify Contract Owners or Contract Owner representatives (who will subsequently request related access changes) of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within 3 days; and
e. Monitor provider compliance with personnel security requirements.

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 Organization will:

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and
b. Notify the individual's chain of command, Human Resources, Helpdesk, the Information Security Office, and other applicable personnel and roles within 72 hours 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)

PS-9: Position Descriptions

The Organization will Incorporate security and privacy roles and responsibilities into organizational position descriptions.

For systems containing Federal Tax Information

PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

PT-1: PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY Policy & Procedures

The Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and/or System-level personally identifiable information processing and transparency Policy & Procedures that:
    a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;

b. Designate the Chief Privacy Officer or his/her designee to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and

c. Review and update the current personally identifiable information processing and transparency:

1. Policy every three years and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
2. Procedures every three years and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

For systems containing Federal Tax Information

PT-2: Authority to Process Personally Identifiable Information

The Organization will:

a. Determine and document the IRC § 6103 section that permits the receipt of personally identifiable information; and
b. Restrict the access of personally identifiable information to only that which is authorized.

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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and/or System-level Risk Assessment Policy & Procedures 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. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Risk Assessment policy and procedures; and

c. Review and update the current Risk Assessment:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and

2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

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

Organizational Systems will:

a. Categorize the system and information it processes, stores, and transmits;
b. Document the security categorization results, including supporting rationale, in the security plan for the system; and
c. Verify that the authorizing official or authorizing official 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 Organization will:

a. Conduct a risk assessment, including:
    1. Identifying threats to and vulnerabilities in the system;
    2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
    3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;
b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;
c. Document risk assessment results in security plans; and risk assessment report;
d. Review risk assessment results annually;
e. Disseminate risk assessment results to the Information Security Office, the Security Operations Center, System Owner, Business Owner, other affected stakeholders, and Organizational leadership; and
f. Update the risk assessment every three years or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

For systems containing Federal Tax Information

RA-3 (enhancement 1): Supply Chain Risk Assessment

The Organization will:

a. Assess supply chain risks associated with Federal Tax Information and
b. Update the supply chain risk assessment every three (3) years, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain

RA-5: Vulnerability Scanning

The Organization will:

a. Monitor and scan for vulnerabilities in the system and hosted applications every 72 hours for system component scans and monthly for hosted application scans and/or randomly in accordance with organization-defined processes and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and

3. Measuring vulnerability impact;
4. Complying with the organization's continuous monitoring program and CMS requirements; and
5. Complying with the required reporting metrics.

c. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities per the schedule defined in SI-2: Flaw Remediation in accordance with an organizational assessment of risk;
e. Share information obtained from the vulnerability monitoring process and control assessments with System Administrators, Development staff, the Security team, and other applicable resources to help eliminate similar vulnerabilities in other systems; and
f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

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

The Organization will update the system vulnerabilities to be scanned daily; prior to a new scan; or when new vulnerabilities are identified and reported.

RA-5 (enhancement 3): Depth and Breadth of Coverage

The organization will define the breadth and depth of vulnerability scanning coverage.

RA-5 (enhancement 4) Discoverable Information:

Determine information about the system that is discoverable and take appropriate corrective actions

RA-5 (enhancement 5): Privileged Access

The Organization will Implement privileged access authorization to information system components for host-based and dynamic web app vulnerability scanning activities.

RA-5 (enhancement 6): AUTOMATED TREND ANALYSES

Compare the results of multiple vulnerability scans using automated mechanisms.

RA-5 (enhancement 8): REVIEW HISTORIC AUDIT LOGS

Review historic audit logs to determine if a vulnerability identified in organizational systems has been previously exploited within a 90-day time period.

For systems containing Federal Tax Information

Implement a vulnerability management process for IT software systems (including wireless networks) to complement their patch management process.

RA-5 HIPAA mapping

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

RA-7: Risk Response

The Organization will Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

For systems containing Federal Tax Information

RA-8: Privacy Impact Assessments

The Organization will Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

RA-9: Criticality Analysis

Organizational Systems will Identify critical system components and functions by performing a criticality analysis for systems, system components, or system services at the implementation phase of the organizational system development life cycle.

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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and/or System-level System & Services Acquisition Policy & Procedures 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. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the System & Services Acquisition policy and procedures; and

c. Review and update the current System & Services Acquisition:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and

2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

SA-2: Allocation of Resources

Organizational Systems will:

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

SA-3: System Development Lifecycle

Organizational Systems will:

a. Acquire, develop, and manage the system using the organizational system development life cycle that incorporates information security and privacy considerations;
b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;
c. Identify 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 Organization:

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

Organizational Systems will Include the following requirements, descriptions, and criteria, explicitly or by reference, using standardized contract language in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;
b. Strength of mechanism requirements;
c. Security and privacy assurance requirements;
d. Controls needed to satisfy the security and privacy requirements.
e. Security and privacy documentation requirements;
f. Requirements for protecting security and privacy documentation;
g. Description of the system development environment and environment in which the system is intended to operate;
h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and
i. Acceptance criteria.

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

Organizational Systems will require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

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

Organizational Systems will require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics;

and/or other applicable controls at a level of detail that will allow the organization to perform risk and security assessments against the system, system component, or system service.

SA-4 (enhancement 8): CONTINUOUS MONITORING PLAN FOR CONTROLS

Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.

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

Organizational Systems will Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

For systems containing Federal Tax Information

SA-4 (enhancement 12): DATA OWNERSHIP

The Organization will:

a. Include organizational data ownership requirements in the acquisition contract; and
b. Require all data to be removed from the contractor's system and returned to the organization within at least 90 days.

For systems containing Federal Tax Information

Information systems that receive, process, store, access, protect and/or transmit FTI must be located, operated, and accessed within the United States. When a contract developer is used, agencies must document, through contract requirements, that all FTI systems (i.e., beyond commercial products used as components) are located within the United States and are developed physically within the United States by United States citizens or those with lawful resident status.

For systems containing Federal Tax Information

In acquiring information technology, agencies must use common security configurations, when applicable, by (a) requiring vendors to configure IT with common security configurations (when available and applicable, e.g., Center for Internet Security benchmarks) prior to delivery or (b) configuring acquired IT to meet agency-tailored, secure parameters (e.g., configurations that meet Publication 1075 and applicable SCSEM requirements) after delivery but prior to deployment.

SA-4 HIPAA Mapping

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

SA-5: System Documentation

Organizational Systems will:

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:
    1. Secure configuration, installation, and operation of the system, component, or service;
    2. Effective use and maintenance of security and privacy functions and mechanisms; and
    3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;
b. Obtain or develop user documentation for the system, system component, or system service that describes:
    1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;
    2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
    3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;
c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take corrective contractual or financial actions in response; and
d. Distribute documentation to System Owners, Organizational leadership, related System Administrators, and other related personnel or roles only as necessary to perform functions or roles.

SA-8: Security and Privacy Engineering Principles

Organizational Systems will apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components:

- Security and Privacy Engineering Principles in line with the Organization's System Development Life Cycle (or one deemed acceptable by the organization); and
- Security and Privacy Engineering Principles in line with the Organization's acceptable technical architecture.

SA-9: External System Services

Organizational Systems will:

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: all security controls made applicable by the information being exported into the system (per applicable Federal laws, State laws, leadership directives, policies, regulations, etc…);
b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: regular CA-2: Security Assessments.

SA-9 (enhancement 1): RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS

The Organization will:

a. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and
b. Verify that the acquisition or outsourcing of dedicated information security services is approved by the Chief Information Security Officer and Organizational Leadership.

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.

For systems containing Federal Tax Information

SA-9 (enhancement 3): ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS

Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: IRS Publication 1075 requirements for information systems that process, store, or transmit FTI.

SA-9 (enhancement 5): PROCESSING, STORAGE, AND SERVICE LOCATION

Restrict the location of information processing; information or data; system services to organization-defined locations (defined in the applicable system security plan and, as applicable to Federal Tax Information, restrict transmission of FTI to The U.S. and territories based on IRS Publication 1075 requirements) based on program requirements or conditions.

For systems containing Federal Tax Information

SA-9 (enhancement 6): ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS

Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.

For systems containing Federal Tax Information

SA-9 (enhancement 8): PROCESSING AND STORAGE LOCATION — U.S. JURISDICTION

Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.

SA-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

Organizational Systems will Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service operation (not necessarily the design; development; implementation; or disposal phases unless necessary);
b. Document, manage, and control the integrity of changes to production configuration items (or configuration items housing production information) under configuration management;
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to Information Security Office, Chief Information Officer, program manager, system owner, information owner, and other individuals and roles as required.

SA-10 (enhancement 1): SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION

The organization will require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.

For systems containing Federal Tax Information

SA-10 (enhancement 3): HARDWARE INTEGRITY VERIFICATION

The Organization will Require the developer of the system, system component, or system service to enable integrity verification of hardware components.

For systems containing Federal Tax Information

SA-10 (enhancement 7): SECURITY AND PRIVACY REPRESENTATIVES

The Organization will require agency designated security and privacy representatives to be included in the configuration change management and control process.

SA-11: Developer Security Testing and Evaluation

Organizational Systems will require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

a. Develop and implement a plan for ongoing security and privacy control assessments;

b. Perform unit; integration; system; and/or regression testing/evaluation as needed at the following depth and coverage: high level design/operation;
c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during testing and evaluation.

SA-11 (enhancement 1): STATIC CODE ANALYSIS

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

SA-11 (enhancement 2): THREAT MODELING AND VULNERABILITY ANALYSES

Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:

a. Uses the following contextual information: information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels;
b. Employs the following tools and methods: dynamic and static application and code scanning tools;
c. Conducts the modeling and analyses at the following level of rigor: moderate level of rigor and detail; and
d. Produces evidence that meets the following acceptance criteria: Meets organizational Security requirements within the Organization's defined tolerance for risk (i.e. Moderate).

For systems containing Federal Tax Information

SA-11 (enhancement 4): Manual Code Reviews

Require the developer of the system, system component, or system service to perform a manual code review of FTI-related applications using the following processes, procedures, and/or techniques: agency-defined manual review processes.

For systems containing Federal Tax Information

SA-11 (enhancement 5): Penetration Testing

Require the developer of the system, system component, or system service to perform penetration testing:

a. At the following level of rigor: at a minimum Whitebox testing; and
b. Under the following constraints: where FTI is processed, stored, or transmitted.

For systems containing Federal Tax Information

SA-11 (enhancement 6): Attack Surface Reviews

Require the developer of the system, system component, or system service to perform attack surface reviews.

SA-11 (enhancement 8): DYNAMIC CODE ANALYSIS

Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

For systems containing Federal Tax Information

SA-15: Development Process, Standards, and Tools

Organizational Systems will:

a. Require the developer of the system, system component, or system service to follow a documented development process that:
    1. Explicitly addresses security and privacy requirements;
    2. Identifies the standards and tools used in the development process;
    3. Documents the specific tool options and tool configurations used in the development process; and
    4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
b. Review the development process, standards, tools, tool options, and tool configurations at a minimum annually to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements IRS Publication 1075 security and privacy requirement.

SA-15 (enhancement 3): Criticality Analysis

Require the developer of the system, system component, or system service to perform a criticality analysis:

a. At the following decision points in the system development life cycle: the agency-defined
b. breadth/depth; and
c. At the following level of rigor: post-design phases of the SDLC.

SA-22: Unsupported System Components

Organizational Systems will:

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or
b. Provide the following options for alternative sources for continued support for unsupported components: in-house support (if available); extended support provided by the vendor (if fiscally responsible), external support provided using refurbished components – all ensuring that no exploitable vulnerabilities exist in the moderate, high, or critical categories; and provide justification and document the approval for the continued use of unsupported system components required to satisfy mission/business needs.

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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and/or System-level System and Communications Protection Policy & Procedures 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;

a. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the System and Communications Protection policy and procedures; and

b. Review and update the current System and Communications Protection:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

SC-2: Application Partitioning

Organizational Systems will separate user functionality, including user interface services, from system management functionality.

For systems containing Federal Tax Information

SC-2 (enhancement 1): Interfaces for Non-Privileged Users

Prevent the presentation of system management functionality at interfaces to non-privileged users

SC-2 HIPAA mapping

HIPAA: 45 C.F.R. §164.312(a)(1)

SC-4: Information in Shared Systems Resources

Organizational Systems will 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

Organizational systems will:

a. Protect Against or Limit the effects of the following types of denial-of-service events: Denial-of-Service and Distributed Denial-of-Service events (as defined in NIST SP 800-61: Computer Security Incident Handling Guide); and
b. Employ the following controls to achieve the denial-of-service objective: deploy technologies in high-availability clusters when available; use distributed, cloud-based reverse proxies when practical; use other manual or automatic communications limiting mechanisms when DoS or DDoS attacks are discovered.

SC-6: Resource Availability

Organizational systems will protect the availability of resources by allocating resources by priority and/or quota.

SC-7: Boundary Protection

Organizational Systems will:

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

3,4,5,7,8,12,13 - CMS only,18; (9,10,11,15,17 - IRS)

SC-7 (enhancement 3): Access Points

Organizational systems will Limit the number of external network connections to the system.

SC-7 (enhancement 4): External Telecommunications Services

Organizational Systems will:

a. Implement a managed interface for each external telecommunication service;
b. Establish a traffic flow policy for each managed interface;
c. Protect the confidentiality and integrity of the information being transmitted across each interface;
d. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
e. Review exceptions to the traffic flow policy quarterly and remove exceptions that are no longer supported by an explicit mission or business need;
f. Prevent unauthorized exchange of control plane traffic with external networks;
g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
h. Filter unauthorized control plane traffic from external networks.

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

Organizational Systems will Deny network communications traffic by default and allow network communications traffic by exception for production organizational systems or non-production systems housing production information.

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

Organizational Systems will prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using organization-controlled security controls or mechanisms similar to those protecting the system.

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

Organizational systems will route internal communications traffic to networks external to the organization (including the internet) through authenticated proxy servers at managed interfaces.

For systems containing Federal Tax Information

SC-7 (enhancement 9): RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC

a. Detect and deny outgoing communications traffic posing a threat to external systems; and
b. Audit the identity of internal users associated with denied communications.

For systems containing Federal Tax Information

SC-7 (enhancement 10): PREVENT EXFILTRATION

a. Prevent the exfiltration of information; and
b. Conduct exfiltration tests semi-annually.

For systems containing Federal Tax Information

SC-7 (enhancement 11): RESTRICT INCOMING COMMUNICATIONS TRAFFIC

Only allow incoming communications from authorized sources to be routed authorized destinations.

SC-7 (enhancement 12): HOST-BASED PROTECTION

Implement host-based boundary protection mechanisms (including firewalls and host-based intrusion detection systems) at system components (where appropriate).

SC-7 (enhancement 13): ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS

Isolate information security tools, mechanisms, and support components from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

For systems containing Federal Tax Information

SC-7 (enhancement 15): NETWORKED PRIVILEGED ACCESSES

Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

For systems containing Federal Tax Information

SC-7 (enhancement 17): AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS

Enforce adherence to protocol formats.

SC-7 (enhancement 18): FAIL SECURE

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

For systems containing Federal Tax Information

(IRS-Defined): Agencies shall implement and manage boundary protection (typically using firewalls) at trust boundaries. Each trust boundary shall be monitored and communications across each boundary shall be controlled.

(IRS-Defined): Agencies must block known malicious sites (inbound or outbound), as identified to the agency from US-CERT, MS-ISAC or other sources, at each Internet Access Point (unless explicit instructions are provided to agencies not to block specific sites). Blocking is to be accomplished within two business days following release of such sites.

SC-7 HIPAA mapping

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

SC-8: Transmission Confidentiality & Integrity

Organizational systems will protect the confidentiality and integrity of transmitted information.

SC-8 (enhancement 1): Cryptographic Protection

Organizational Systems will Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

SC-8 (enhancement 2): PRE- AND POST-TRANSMISSION HANDLING

Maintain the confidentiality & integrity of information during preparation for transmission and during reception.

For systems containing Federal Tax Information

(IRS-Defined): Agencies shall ensure appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed over video and voice telecommunication and teleconferences.

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

Organizational Systems will terminate the network connection associated with a communications session at the end of the session or:

- Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and
- Forcibly disconnects:
    - inactive remote client-based connections (including VPN connections) after thirty (30) minutes or less of inactivity,
    - communications sessions (including stateful firewall sessions) after 30 minutes of inactivity.

SC-10 HIPAA mapping

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

SC-12: Cryptographic Key Establishment and Management

Organizational Systems will Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: adhering to organizational key generation, distribution, storage, access, and destruction processes in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

SC-12 (enhancement 2): SYMMETRIC KEYS

Produce, control, and distribute symmetric cryptographic keys using NIST FIPS-validated key management technology and processes.

SC-12 (enhancement 3): ASYMMETRIC KEYS

Produce, control, and distribute asymmetric cryptographic keys using one or more of the following: NSA-approved key management technology and processes; prepositioned keying material; DoD-approved or DoD-issued Medium Assurance PKI certificates; DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements.

SC-13: Cryptographic Protection

Organizational Systems will:

a. Determine the organization-defined cryptographic uses as – cryptography will be used to protect sensitive information and organizational intellectual property; and
b. Implement the following types of cryptography required for each specified cryptographic use: cryptography equal in strength to the latest FIPS 140 specifications.

SC-15: Collaborative Computing Devices and Applications

Organizational Systems will:

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: troubleshooting of or with collaborative equipment (individuals potentially observed by the remote collaborative equipment must be notified ahead of time); and
b. Provide an explicit indication of use to users physically present at the devices.

For systems containing Federal Tax Information

SC-15 (enhancement 4): Explicitly Indicate Current Participants

Provide an explicit indication of current participants in meetings that involve FTI.

SC-17: Public Key Infrastructures

Organizational Systems will:

a. Issue public key certificates under a standardized organizational certificate policy (when published by an organization-owned Certificate Authority) or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

SC-18: Mobile Code

Organizational Systems will:

a. Define acceptable and unacceptable mobile code and mobile code technologies; and
b. Authorize, monitor, and control the use of mobile code within the system.

For systems containing Federal Tax Information

SC-18 (enhancement 1): Identify Unacceptable Code and Take Corrective Actions

Identify unacceptable mobile code and take corrective actions.

For systems containing Federal Tax Information

SC-18 (enhancement 2): Acquisition, Development and Use

Verify that the acquisition, development, and use of mobile code to be deployed in the system meets IRS Publication 1075 requirements.

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

Organizational Systems will:

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

For systems containing Federal Tax Information

SC-20 (enhancement 2): Data Origin and Integrity

Provide data origin and integrity protection artifacts for internal name/address resolution queries.

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

Organizational Systems will request and perform 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

Organizational Systems will Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

SC-23: Session Authenticity

Organizational Systems will protect the authenticity of communications sessions.

For systems containing Federal Tax Information

SC-23 (enhancement 1): Invalidate Session Identifies at Logout

Invalidate session identifiers upon user logout or other session termination.

For systems containing Federal Tax Information

SC-23 (enhancement 3): Unique System-Generate Session Identifiers

Generate a unique session identifier for each session with session with agency-defined randomness requirements and recognize only session identifiers that are system-generated.

For systems containing Federal Tax Information

SC-23 (enhancement 5): Allowed Certificate Authorities

Only allow the use of agency-defined certificate authorities for verification of the establishment of protected sessions.

SC-28: Protection of Information at Rest

Organizational Systems will Protect the confidentiality and integrity of the following information at rest: sensitive information or organizational intellectual property.

SC-28 (enhancement 1): Cryptographic Protection

Organizational Systems will Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on organization-owned portable/removable storage, storage media in system components (i.e. workstations and servers), and other applicable storage media: sensitive information or organizational intellectual property.

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

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

SC-32: System Partitioning

Partition the system into system components residing in separate physical or logical domains or environments based on organization-defined circumstances for physical or logical separation of components.

SC-35: External Malicious Code Identification

Organizational systems will include systems components that proactively seek to identify network-based malicious code or malicious websites.

SC-39: Process Isolation

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

For systems containing Federal Tax Information

SC-45: System Time Synchronization

Synchronize system clocks within and between systems and system components.

SC-23 (enhancement 5): Synchronization with Authoritative Time Source:

a. Compare the internal system clocks daily with an agency-defined authoritative time source; and
b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than agency-defined time period.

For systems connecting to the CMS Hub

SC-ACA-1: Electronic Mail:

Controls shall be implemented to protect sensitive information that is sent via email.

SC-ACA-2: FAX Usage:

1. If PII is allowed to be included with fax communications, the organization establishes policies and procedures for handling fax transmissions.
2. The organization must follow specific precautions and Implementation Standards when performing fax transmission of PII:
    1. Transmit PII only to an authorized recipient.

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 Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and/or System-level System & Information Integrity Policy & Procedures that:
    c) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    d) 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. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the System & Information Integrity policy and procedures; and

c. Review and update the current System & Information Integrity:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

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

Organizational Systems will:

a. Identify, report, and correct information system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates 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. Critical – 15 calendar days
  ii. High – 30 calendar days
  iii. Moderate/Medium – 90 calendar days
  iv. Low – 365 calendar days

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

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

Organizational Systems will Determine if system components have applicable security-relevant software and firmware updates installed using host management software or vulnerability scanning software with scans being performed at a minimum every 72 hours, and for hosts containing Federal Tax Information, every 24 hours for networked workstations and malicious code protection.

For systems containing Federal Tax Information

SI-2 (enhancement 3): Time to Remediate Flaws and Benchmarks for Corrective Actions
Organizational systems will:

a. Measure the time between flaw identification and flaw remediation; and
b. Establish the following benchmarks for taking corrective actions: Agency defined based on criticality.

For systems containing Federal Tax Information

SI-2 (enhancement 4): Automated Patch Management Tools

Employ automated patch management tools to facilitate flaw remediation to all FTI systems that includes but not limited to mainframes, workstations, applications, and network components.

For systems containing Federal Tax Information

SI-2 (enhancement 5): Automatic Software and Firmware Updates

Install security-relevant software and firmware updates automatically to all FTI systems.

For systems containing Federal Tax Information

SI-2 (enhancement 6): Removal of Previous Versions of Software and Firmware

Remove previous versions of security relevant software and firmware components after updated versions have been installed.

For systems containing Federal Tax Information

IRS Defined: The agency shall ensure that, upon daily power up and connection to the agency's network, workstations (as defined in policy and including remote connections using government furnished equipment) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than once every 24 hours (excluding weekends, holidays, etc.)

SI-2 HIPAA mapping

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

SI-3: Malicious Code Protection

Organizational Systems will:

a. Implement signature based and heuristic/non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
c. Configure malicious code protection mechanisms to:
    1. Perform periodic scans of the system at least once every 12 hours and real-time scans of files from external sources at the endpoint and network entry and exit points (where possible) as the files are downloaded, opened, or executed in accordance with organizational policy; and
    2. Quarantine malicious code; take additional containment actions if necessary; and send alert to the Security Operations Center and System Administrators in response to malicious code detection; and
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

For systems containing Federal Tax Information

IRS Defined: All removable media must be scanned for malicious code upon introduction of the media into any system on the network and before users may access the media.

For systems containing Federal Tax Information

IRS Defined: Not less than daily, the agency shall check for updates to malicious code scanning tools, including anti-virus (AV) and anti-spyware software and intrusion detection tools and when updates are available, implement on all devices on which such tools reside.

SI-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

Organizational Systems will:

a. Monitor the system to detect:
    1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives:
        - near real-time discovery of threats & threat actors focusing activites on organizational assets;
        - determine and nullify ransomware attacks prior to detonation;
        - determine & nullify botnet instantiation within organizational assets;
        - determine & nullify advanced persistent threat actors early in the attack chain
        - other scenarios negatively impactful to the organization's information assets; and
    2. Unauthorized local, network, and remote connections;
b. Identify unauthorized use of the system through the following techniques and methods:
    - Anomalous activity detections;
    - Remote Access monitoring;
    - Monitoring for unauthorized Data Exfiltration and/or encryption;
    - Other techniques and methods useful in identifying unauthorized use; and
c. Invoke internal monitoring capabilities or deploy monitoring devices:
    1. Strategically within the system to collect organization-determined essential information; and
    2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Analyze detected events and anomalies;
e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
f. Obtain legal opinion regarding system monitoring activities; and
g. Provide reduced detail summary reports to the Security Team, the Security Operations Center leadership, System Owner, and Organizational at least every two weeks and as needed in special circumstances.

SI-4 (enhancement 1): SYSTEM-WIDE INTRUSION DETECTION SYSTEM

Organizational systems will connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

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

Organizational Systems will employ automated tools and mechanisms to support near real-time analysis of events.

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

Organizational Systems will:

a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
b. Monitor inbound and outbound communications traffic in as near real-time as possible for unusual or unauthorized activities or conditions.

SI-4 (enhancement 5): System Generated Alerts

Organizational Systems will alert the Security Operations Center, System Administrators, and other roles and personnel as needed when the following system-generated indications of compromise or potential compromise occur: presence of malicious code, unauthorized export of information, signaling to an external information system, or potential intrusions.

For systems containing Federal Tax Information

SI-4 (enhancement 10): VISIBILITY OF ENCRYPTED COMMUNICATIONS

Make provisions so that agency-defined encrypted communications traffic is visible to agency-defined system monitoring tools and mechanisms.

For systems containing Federal Tax Information

SI-4 (enhancement 11): ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES

Analyze outbound communications traffic at the external interfaces to the system and selected agency-defined interior points within the system to discover anomalies.

For systems containing Federal Tax Information

SI-4 (enhancement 12): AUTOMATED ORGANIZATION-GENERATED ALERTS

Alert agency-defined personnel or roles using automated mechanisms when the following indications of inappropriate or unusual activities with security or privacy implications occur: agency-defined activities that trigger alerts.

SI-4 (enhancement 13): ANALYZE TRAFFIC AND EVENT PATTERNS

Organizational systems will:

a. Analyze communications traffic and event patterns for the system;
b. Develop profiles representing common traffic and event patterns; and
c. Use the traffic and event profiles in tuning system-monitoring devices.

For Systems connecting to the CMS Hub

SI-4 (enhancement 14): WIRELESS INTRUSION DETECTION

Organizational systems will employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

For Systems connecting to the CMS Hub

SI-4 (enhancement 16): CORRELATE MONITORING INFORMATION

Correlate information from monitoring tools and mechanisms employed throughout the system.

For systems containing Federal Tax Information

SI-4 (enhancement 18): ANALYZE TRAFFIC AND COVERT EXFILTRATION

Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information at agency-defined interior points within the system.

For Systems connecting to the CMS Hub

SI-4 (enhancement 23): HOST-BASED DEVICES

Implement the following host-based monitoring mechanisms at all systems, appliance, devices, services, and applications: agency-defined host-based monitoring mechanisms from multiple product developers or vendors.

For systems containing Federal Tax Information

SI-4 (enhancement 24): INDICATORS OF COMPROMISE

Discover, collect, and distribute to organization-defined personnel or roles, indicators of compromise provided by government and non-government sources.

For systems containing Federal Tax Information

IRS-Defined: All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO.

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-5: Security Alerts, Advisories, and Directives

Organizational Systems will:

a. Receive system security alerts, advisories, and directives from the organizational Security Operations Center, US-CERT, MS-ISAC, and DHS CISA on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate security alerts, advisories, and directives to individuals whose roles can benefit from such information, all organizational personnel (when applicable), and/or organizational vendors affected by such information; and
d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

For systems connecting to the CMS Hub

SI-6: SECURITY AND PRIVACY FUNCTION VERIFICATION

a. Verify the correct operation of organization-defined security and privacy functions;
b. Perform the verification of the functions specified in SI-6a upon system startup, restart, and; upon command by user with appropriate privilege; no less than once per month;
c. Alert System Administrators and Security Operations Center Personnel to failed security and privacy verification tests; and
d. Shut the system down; Restart the system; or quarantine the system when anomalies are discovered.

SI-7: Software, Firmware, and Information Integrity

Organizational Systems will:

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: software and firmware on production systems and system components; and sensitive information or organizational intellectual property; and
b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: restore from backups when possible, replace hardware components if necessary to mitigate impacted firmware; reinstall software when backup restoration is ineffective for applications, or other actions as necessary.

SI-7 (enhancement 1): Integrity checks

Organizational Systems will Perform an integrity check of software, firmware, and information at system startup, and/or during transitional states, and after significant cyber security events; at least quarterly.

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

Organizational Systems will Incorporate the detection of the following unauthorized changes into the organizational incident response capability:

- Password changes from non-organizational sources
- Data deletion from production data or databases
- File-based or file-less malware being instantiated on a system component/host
- Unauthorized attempts at file or data exfiltration or encryption
- Other security-relevant changes to the system
- Unauthorized elevation of system privileges

For systems containing Federal Tax Information

SI-7 (enhancement 10): Integration of Detection and Response

Implement the following mechanisms to protect the integrity of boot firmware in system where FTI is accessed, processed, stored, and transmitted: verifying the checksum of downloaded firmware.

SI-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

Organizational Systems will :

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

SI-8 (enhancement 2): Automatic Updates

Organizational Systems will Automatically update spam protection mechanisms at least quarterly.

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

Organizational Systems will check the validity of the following information inputs: all information inputs.

SI-11: Error Handling

Organizational Systems will:

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 System Administrators, Developers, or other support personnel only as needed.

SI-11 HIPAA mapping

HIPAA: 45 C.F.R. §164.308(a)(3)(i)

SI-12: Information Handling and Retention

Organizational Systems will manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

For systems containing Federal Tax Information

SI-12 (enhancement 2): Minimize Personally identifiable Information in Testing, Training, and Research:

Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: Submission of the DTR form for review and approval by IRS Office of Safeguards.

SI-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

Organizational Systems will Implement the following controls to protect the system memory from unauthorized code execution: data execution prevention (either hardware-enforced or software-enforced) or address space layout randomization.

Supply Chain Risk Management

SR-1: Policy and Procedures

The Organization will:

a. Develop, document, and disseminate to organizational leadership, system owners, and applicable stakeholders:

1. Organization-level and/or System-level Supply Chain Risk Management Policy & Procedures that:
    a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the Supply Chain Risk Management policy and the associated Supply Chain Risk Management controls;

b. Designate the Chief Information Security Officer or his/her designee to manage the development, documentation, and dissemination of the Supply Chain Risk Management policy and procedures; and

c. Review and update the current Supply Chain Risk Management:

1. Policy Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments; and
2. Procedures Annually and following catastrophic cyber security events, substantial organizational changes, or the discovery of significant problems identified during policy implementation or control assessments.

SR-2: Supply Chain Risk Management Plan

The Organization will:

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: organizational system or system components housing sensitive information or organizational intellectual property;

b. Review and update the supply chain risk management plan every annually or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

SR-2 (1): Establish SCRM Team

The Organization will Establish a supply chain risk management team consisting of Organizational Leadership, System Owners, and the Security Team to lead and support the following SCRM activities: provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems.

SR-3: Supply Chain Controls and Processes

The Organization will:

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of organizational system or system components in scope for SCRM activities in coordination with Organizational Leadership, System Owners, and the Security Team;
b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: Security Assessments, Risk Assessments, contractual obligations (to meet organizational security policy requirements): organization involvement in vendor vulnerability management and PoA&M process; and other applicable organizational supply chain processes and controls; and
c. Document the selected and implemented supply chain processes and controls in security and privacy plans or supply chain risk management plan.

For systems containing Federal Tax Information

SR-3 (enhancement 2): Limitation of Harm

Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: agency-defined controls.

For systems containing Federal Tax Information

SR-3 (enhancement 3): Sub-Tier Flow Down

Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.

SR-5: Acquisition Strategies, Tools, and Methods

The Organization will employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: Security Assessments, Risk Assessments, contractual obligations (to meet organizational security policy requirements); organization involvement in vendor vulnerability management and PoA&M process.

SR-6: Supplier Assessments and Reviews

The Organization will Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide annually.

SR-8: Notification Agreements

The Organization will Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the: notification of supply chain compromises; vulnerability scan results, and the results of assessments or audits.

SR-10: Inspection of Systems or Components

The Organization will Inspect the following systems or system components as needed at random (but at least annually); or upon indications of need for inspection to detect tampering: systems or system components housing sensitive information or organizational intellectual property.

SR-11: Component Authenticity

The Organization will:

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and
b. Report counterfeit system components to the source of counterfeit component; applicable external reporting organizations; Systems Owners, the Security Team, and Organizational Leadership.

SR-11 (1): Anti-counterfeit Training

The Organization will Train system engineers, ISSO(s), System Owners, and other applicable personnel to detect counterfeit system components (including hardware, software, and firmware).

SR-11 (2): Configuration Control for Component Service and Repair

The Organization will Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: system components containing sensitive information or organizational intellectual property.

SR-12: Component Disposal

The Organization will dispose of sunsetted vendor data, documentation, tools, or system components (when necessary) using the following techniques and methods: Purge or Destroy methods as described in the most recent revision of NIST 800-88.

Conclusion

Treating information and IT assets as strategic resources allows Medicaid to 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 16th day of September, 2022.

Mason L. Tanaka

Alabama Medicaid Agency, Chief Information Officer