OREGON | Office of the State
Chief Information Officer

OREGON
Enterprise
Security
Office

2019
Statewide Information and Cyber Security Standards

Initial Release
Version 1.0

June 24, 2019

Level 1, Published

AUTHORITY

The Oregon Office of the State Chief Information Officer (OSCIO) has the responsibility for developing and overseeing the implementation of statewide information and cyber security standards, and policies on information security, under the authority of Oregon Revised Statute 276A.300. The Enterprise Security Office (ESO) operates as part of OSCIO and is responsible for creation and maintenance of the Statewide Information and Cyber Security Standards.

APPROVAL

6-24-19

Terrence Woods
State of Oregon Chief Information Officer

Date

6/14/19

Annalise Famiglietti
State of Oregon Chief Information Security Officer (Interim)

Date

ACKNOWLEDGEMENTS

The 2019 Statewide Information and Cyber Security Standards Workgroup

Core Workgroup Members

Steve Harvath, Oregon Enterprise Security Office, Co-Chair
Norm Walters, Oregon Department of Employment, Co-Chair
Brian Goergen, Oregon Department of Transportation
Monte Hogan, Oregon Emergency Management
Bill Kellogg, Oregon Department of Corrections
Dave Komanecky, Oregon Enterprise Technology Services
Anthony Mingus, Oregon Department of Justice
Paul Musack, Oregon State Police
Skip Pikl, Oregon Department of Fish and Wildlife
Karina Stewart, Oregon Department of Transportation
Greg Verharst, Oregon Department of State Lands

Additional Contributors

Cinnamon Albin, Vince Almberg, Kristine Cornett, Nick Ettel, Teresa Furnish, Mark Johnston, Steve Ketchum, Uma Krishnan, Dave McMorries, Mike Poverud, Jaya Srinivasan, Dustin VanElverdinghe

Table of Contents

EXECUTIVE SUMMARY

The Office of the State Chief Information Officer (OSCIO) has established the following Statewide Information and Cyber Security Standards. These Standards facilitate the development, implementation, and operation of secure information and process control systems by establishing a minimum set of security controls for accessing, processing, and storing information at defined information asset classification levels. These Standards facilitate a consistent, comparable, and repeatable approach for applying security controls. The controls specified in this document can be referenced by state and agency policies and procedures instead of redefining the same controls within an individual policy or procedure.

OSCIO has the responsibility for developing and overseeing the implementation of statewide information and cyber security standards, and policies on information security, under the authority of Oregon Revised Statute 276A.300. These Standards address diverse requirements derived from mission and business needs, laws, Executive Orders, directives, regulations, policies, standards, and guidelines. These Standards apply to systems, policies, and procedures within all Executive Branch agencies. Agencies are responsible for complying with these Standards and ensuring that third parties acting on behalf of agencies have formal agreements that guarantee compliance with these Standards.

These Standards provide a catalog of security controls for State of Oregon information systems to protect state operations, assets, and individuals from a diverse set of threats including malicious acts, natural disasters, structural failures, information system errors and human errors. These Standards support and align with the published Statewide Information Security Plan and applicable statewide policies, including the relevant control families of the National Institute of Standards and Technology Special Publication 800-53 Revision 5 (NIST SP 800-53 R5).

Individual controls within these Standards specify techniques associated with protecting and securely providing access to the State's information systems. Agencies may elect to exceed these Standards to achieve their organizational security goals and requirements by applying additional controls. The controls documented in these standards are interdependent and are intended to be implemented in their entirety.

These standards have been developed using reference documents from the following resources:

- National Institute of Standards and Technology (NIST)
- Center for Internet Security (CIS)
- Federal, State, and Local Statues and Rules

The NIST Glossary of Key Information Security Terms is used as the standard reference for terms utilized throughout this document.

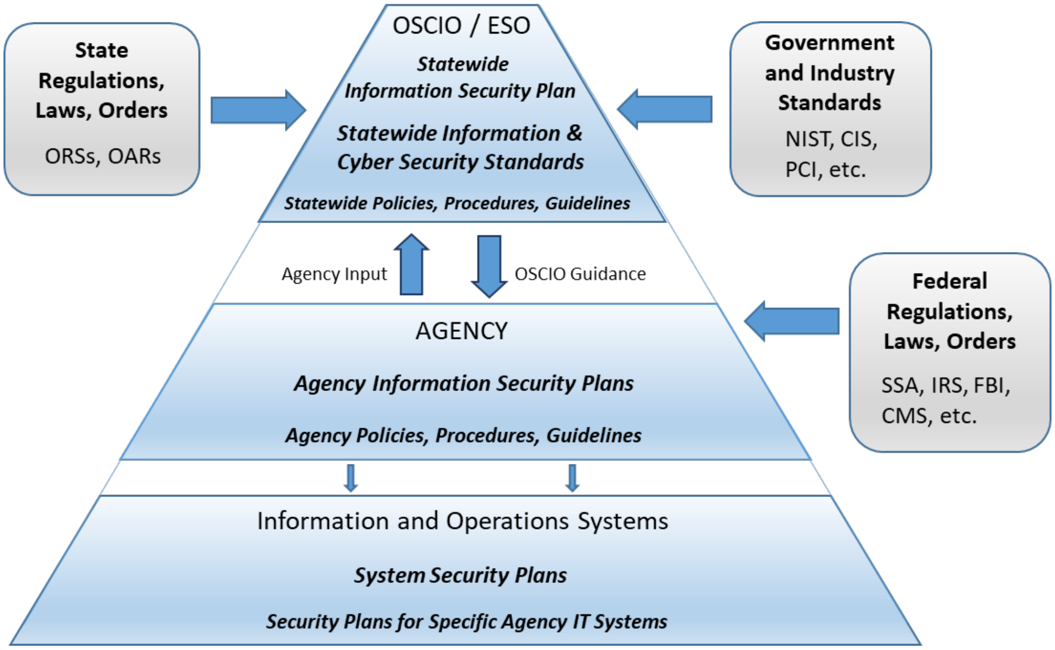
In circumstances where these Standards cannot be implemented, agencies must document deviations and indicate the compensating controls that have been applied to adequately protect systems or information. A deviation document must be signed by the agency head and approved by OSCIO.

ABOUT THIS DOCUMENT

This document is one component of the Statewide Information and Cyber Security Program for the State of Oregon. Components of the security program are detailed in the following documents:

- Statewide Security Plan
- Statewide Information and Cyber Security Standards (this document)
- Statewide Information and Cyber Security Policies
- Agency Information and Cyber Security Plans
- Agency Information and Cyber Security Policies
- System Security Plans

State of Oregon
Information and Cyber Security Program
Documentation Hierarchy


State Regulations, Laws, Orders
ORSs, OARs
OSCIO / ESO
Statewide Information Security Plan
Statewide Information & Cyber Security Standards
Statewide Policies, Procedures, Guidelines
Government and Industry Standards
NIST, CIS, PCI, etc.
Agency Input
OSCIO Guidance
Federal Regulations, Laws, Orders
SSA, IRS, FBI, CMS, etc.
AGENCY
Agency Information Security Plans
Agency Policies, Procedures, Guidelines
Information and Operations Systems
System Security Plans
Security Plans for Specific Agency IT Systems

The controls selected for these standards constitute the minimum set of controls necessary to meet the requirements for information system and organizational operations within the State of Oregon. These standards provide a set of common management, operational, and technical security controls that must be implemented. The inclusion of the control in a policy (typically by reference) officially makes the control a 'common control' for the State of Oregon (State policies) or for the specific agency (Agency policies).

The Control Identifiers defined in this document can also be referenced as common controls when a System Security Plan is created for a specific Information system.

The Oregon Statewide Information Asset Classification Policy (107-004-050) requires each agency to identify and classify its information assets for the purpose of defining the value, criticality, sensitivity, and legal implications of those assets.

The system security categorization process is carried out by the System Owner and the Information Owner, in collaboration with other appropriate organizational personnel (e.g. the Authorizing Official (or designee), Information System Auditor, Business Information Security Officer, Information System Specialist, etc.). The security categorization must be consistent with the potential impact and magnitude of harm to agency mission and business functions that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of State of Oregon information and systems.

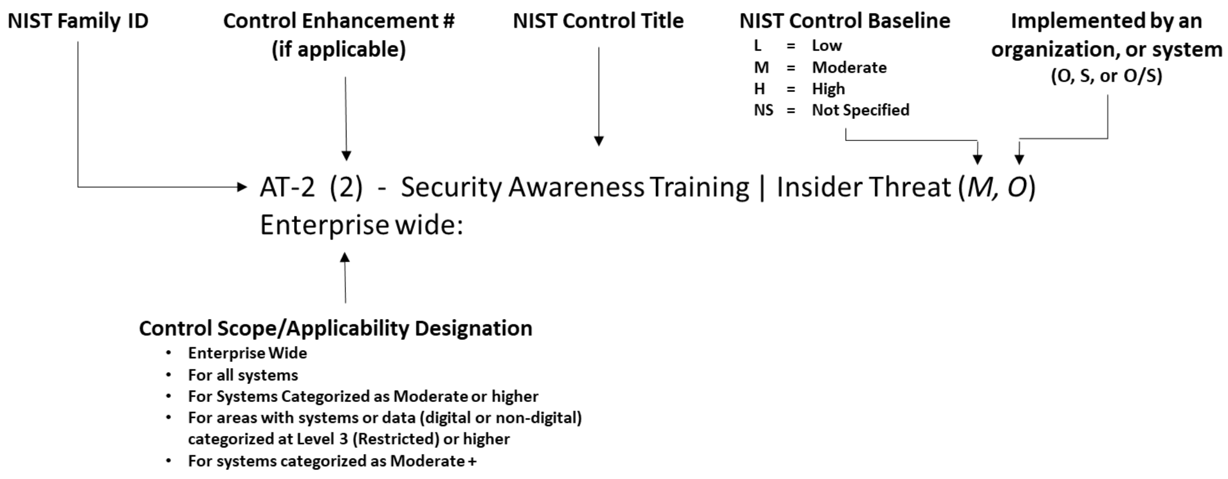
This document designates the scope and applicability of listed controls as follows:

Control Scope/Applicability	**NIST Control Tailoring**
• For non-system-specific controls	
○ Enterprise Wide	Low + Discretionary
○ For areas with systems or data (digital or non-digital) categorized at Level 3 (restricted) or higher	Moderate + Discretionary
• For system-specific controls	
○ All Systems	Low + Discretionary
○ For Systems categorized as Moderate or higher	Moderate + Discretionary
○ For Systems categorized as Moderate +	Moderate + Further Discretionary

The system security categorization is dependent on the data classification as follows:

State of Oregon Data Classification	**Use Controls with the following Control Scope/Applicability**
• Level 1, Published	For all systems / Enterprise wide
• Level 2, Limited	For all systems / Enterprise wide
• Level 3, Restricted	Moderate
• Level 4, Critical	Moderate +

The structure of the control labeling used throughout this document is as follows:


NIST Family ID
Control Enhancement # (if applicable)
NIST Control Title
NIST Control Baseline
L = Low
M = Moderate
H = High
NS = Not Specified
Implemented by an organization, or system (O, S, or O/S)
AT-2 (2) - Security Awareness Training | Insider Threat (M, O)
Enterprise wide:
Control Scope/Applicability Designation
• Enterprise Wide
• For all systems
• For Systems Categorized as Moderate or higher
• For areas with systems or data (digital or non-digital) categorized at Level 3 (Restricted) or higher
• For systems categorized as Moderate +

There are also references to CIS V7.1 embedded within the controls in this document where a specific control item aligns with the referenced CIS V7.1 control. These references have the form '(CIS-x.x)'.

STATEWIDE SECURITY CONTROLS

ACCESS CONTROL - AC

AC-2 - Account Management (L, *O*)

For all systems

a. Define and document the types of accounts to support organizational missions and business functions (CIS-4.1);
b. Assign Account Managers for system accounts;
c. Establish conditions for group and role membership;
d. Specify authorized users of the system, group and role membership, and access authorizations (i.e. privileges) for each account, and maintain an inventory of all accounts organized by the authentication system (CIS-16.6);
e. Approve requests to create system accounts;
f. Create, enable, modify, disable, and remove system accounts in accordance with documented account management procedures;
g. Monitor the use of system accounts, and alert when users deviate from normal login behavior (e.g. time of day, workstation location, duration, etc.) (CIS-16.13);
h. Notify Account Managers:
    1. When accounts are no longer required;
    2. When user employment is terminated or transferred; and
    3. When individual system usage or need-to-know changes;
i. Authorize access to the system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. Applicable federal and state laws and regulations;
j. Review accounts for compliance with account management requirements; at a minimum accounts must be reviewed annually for user accounts, and semi-annually for privileged accounts;
k. Establish a process for reissuing shared / group account credentials when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.

NOTE: System account types include, for example, individual, shared, group, application, guest, anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

AC-2(1) - Account Management | Automated System Account Management (M, O)

For systems categorized as Moderate, or higher

a. Employ automated mechanisms to support the management of system accounts; and
b. Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor (CIS-16.7).

NOTE: Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

AC-2(2) - Account Management | Removal of Temporary / Emergency Accounts (M, S)

For systems categorized as Moderate, or higher

Automatically disable temporary accounts upon completion of use, or pre-defined expiration time, and disable emergency accounts within one year.

AC-2(3) - Account Management | Disable Inactive Accounts (M, S)

For systems categorized as Moderate, or higher

a. Automatically disable system accounts when the account:
    1. Has expired (CIS-16.10);

2. Is no longer associated with a user (CIS-16.8);
3. Is in any way in violation of organizational policy;
4. Is no longer used by applications, services, or the system (CIS-16.8); and
5. Has been inactive for 60 days (CIS-16.9).

AC-2(4) - Account Management | Automated Audit Actions (M, S)
For systems categorized as Moderate, or higher

Automatically audit account creation, modification, enabling, disabling, and removal actions, and notify appropriate personnel as defined in the applicable System Security Plan (CIS-14.9).

AC-2(10) - Account Management | Shared and Group Account Credential Change (M, O)
For systems categorized as Moderate, or higher

Change shared and group accounts credentials when members leave the group.

AC-2(12) - Account Management | Account Monitoring for Atypical Usage (H, O)
For systems categorized as Moderate +:

a. Monitor system accounts for atypical usage; and
b. Report atypical usage of system accounts to appropriate agency personnel as defined in the applicable system security plan (CIS-16.13).

NOTE: Atypical usage includes, for example, accessing systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations.

AC-2(13) - Account Management | Disable Accounts for High-Risk Individuals (M, O)
For systems categorized as Moderate, or higher

Disable system accounts within one hour, where users pose a significant risk to the organization.

NOTE: Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Close coordination and cooperation among authorizing officials, system administrators, and human resource managers is essential for timely execution of this control enhancement.

AC-3 - Access Enforcement (L*, S*)

For all systems

a. Enforce approved authorizations for logical access to information and system resources in accordance with statewide and agency access control policies, procedures, and standards, including applicable federal and state laws, and administrative rules; and
b. Automated tools must be used to enforce access controls to information, even when data is copied off a system (CIS-14.7).

AC-3(7) - Access Enforcement | Role-Based Access Control (NS, O/S)
For systems categorized as Moderate, or higher

Enforce a role-based access control policy over defined subjects and objects, and control access based upon user job classification, position description, function, and need to know.

AC-4 - Information Flow Enforcement (M*, S*)

For systems categorized as Moderate, or higher

a. Enforce approved authorizations for controlling the flow of information within the system, and between interconnected systems based on agency-defined information flow control policies; and
b. Document all configuration rules that allow traffic to flow through network devices. Documentation must be managed in a configuration management system with: a specific business reason for each rule; a

specific individual's name responsible for that business need; and an expected duration of the need (CIS-11.2).

AC-5 - Separation of Duties (M, *O*)

For systems categorized as Moderate, or higher

a. Separate personnel duties to minimize the potential for abuse of authorized privileges and risk of malevolent activity without collusion;
   1. Developers must not have unmonitored access to production environments (CIS-18.9);
b. Document separation of duties, including roles and permissions; and
c. Define system access authorizations in support of separation of duties.

NOTE: For example, personnel performing system administration duties must be separate from personnel performing system audit duties. Personnel performing system development duties must be separate from personnel performing system change duties. Personnel performing system security duties must be separate from personnel performing system security administration.

AC-6 - Least Privilege (M, *O*)

For all systems

Employ the principle of least privilege, allowing only authorized access for users, or processes acting on behalf of users, which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions (CIS-4.1).

AC-6(1) - Least Privilege | Authorize Access to Security Functions (M, O)

For all systems

a. Explicitly authorize access to administrative privileges, including security functions and security relevant information (CIS-4.1); and
b. Establish procedures to maintain documentation of privileged access, including any elevated privileges, and privileges that provide administrative access to network devices, operating systems, software application capabilities, or scripting tools (CIS-4.7).

AC-6(2) - Least Privilege | Non-privileged Access for Non-privileged Functions (M, O)

For all systems

Require that users of system accounts, or roles, with access to privileged or administrative functions, use non-privileged accounts or roles when accessing systems for non-privileged, or non-security functions (CIS-4.3).

AC-6(5) - Least Privilege | Privileged Accounts (M, O)

For all systems

Restrict privileged accounts to authorized individuals with a need for elevated privileges (CIS-4.1).

AC-6(7) - Least Privilege | Review of User Privileges (L, O)

For all systems

a. Ensure that privileges assigned to users are reviewed to validate the need for such privileges:
   1. Initially upon hire;
   2. Any time assigned job duties change;
   3. Any time there is a change in job position (e.g. promotion, demotion, or transfer to another division or section within the Agency – see also: Personnel Transfer – PS-5); and
   4. Annually thereafter; and
b. Reassign or remove privileges as necessary, to correctly reflect organizational mission and business needs.

AC-6(9) - Least Privilege | Auditing Use of Privileged Functions (L, S)

For all systems

Audit the execution of privileged functions.

AC-6(10) - Least Privilege | Prohibit Non-privileged Users From Executing Privileged Functions (M, S)

For all systems

Prevent non-privileged users from executing privileged functions; including disabling, circumventing, or altering implemented security safeguards and countermeasures.

AC-7 - Unsuccessful Logon Attempts (L*, S*)

For all systems

a. Enforce a limit of no greater than five consecutive invalid logon attempts by a user during a 120-minute time period; and
b. Automatically lock the account for a period of at least 15 minutes.

AC-7(2) - Unsuccessful Logon Attempts | Purge / Wipe Mobile Device (M, S)

Enterprise wide

Configure mobile devices to purge or wipe stored information after 10 consecutive unsuccessful logon attempts.

NOTE: This control applies only to mobile devices for which a logon occurs. The logon is to the mobile device, not to any one account on the device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. **Laptop computers are exempt from this requirement**.

AC-8 - System Use Notification (L*, O/S*)

For all systems

a. Display to users an approved system use notification that provides privacy and security notices consistent with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance. This must occur prior to granting access to the system. The system use notification message shall, at a minimum, provide the following information:
    1. The user is accessing a restricted system;
    2. System usage may be monitored, recorded, and subject to audit;
    3. Unauthorized use of the system is prohibited and may be subject to criminal, civil, or administrative penalties; and
    4. Use of the system constitutes consent to monitoring and recording;
b. Retain the notification message until users acknowledge the usage conditions and take explicit actions to log onto, or further access, the system; and
c. For publicly accessible systems:
    1. Display system use notification before granting access;
    2. Display references, if any, to monitoring, recording, or auditing that are consistent with the privacy accommodations for such systems that generally prohibit monitoring, recording, or auditing activities; and
    3. Include a description of the authorized uses of the system.

AC-11 - Device Lock (M*, S*)

For all systems

a. Automatically initiate a device lock after 15 minutes of inactivity (CIS-16.11); and
b. Retain the device lock until the authorized user reestablishes access using identification and authentication procedures.

AC-11(1) - Device Lock | Pattern Hiding Displays (M, S)
For all systems

Conceal, via the device lock, information previously visible on the display, with a publicly viewable image. The pattern-hiding display can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the caveat that controlled unclassified information is not displayed.

AC-11(2) - Device Lock | Require User-Initiated Lock (NS, O)
Enterprise wide

Require the user to initiate a device lock before leaving the system unattended.

AC-12 - Session Termination (M*, S*)

For systems categorized as Moderate, or higher

Automatically terminate user sessions after 30 minutes of inactivity, unless otherwise defined in the applicable system security plan.

AC-14 - Permitted Actions without Identification or Authentication (L*, O*)

For all systems

a. Identify specific user actions that can be performed on the system without identification or authentication consistent with agency missions and business functions; and
b. Document and provide supporting rationale in system security plans for user actions that do not require identification and authorization.

NOTE: This control addresses situations in which organizations determine that no identification or authentication is required in organizational systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible systems, when individuals use mobile phones to receive calls, or when facsimiles are received. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred.

AC-17 - Remote Access (L*, O*)

For all systems

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

For systems categorized as Moderate, or higher

b. Explicitly authorize and document remote access to internal systems prior to allowing such connections. Documentation must include the purpose for authorized remote access, conditions, duration, and approved connection methods; and
c. Require the use of multifactor authentication for all remote access.

AC-17(1) - Remote Access | Automated Monitoring and Control (M, S)
For systems categorized as Moderate, or higher

a. Monitor and control remote access methods; and
b. Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network device (CIS-12.12).

AC-17(2) - Remote Access | Protection of Confidentiality / Integrity Using Encryption (M, S)
For systems categorized as Moderate, or higher

Implement a FIPS 140-2 validated cryptographic mechanism to protect the confidentiality and integrity of remote access sessions and information (CIS-12.11).

AC-17(3) - Remote Access | Managed Access Control Points (M, S)
For systems categorized as Moderate, or higher

Route all remote accesses through a limited number of managed network access control points.

AC-17(4) - Remote Access | Privileged Commands / Access (M, O)
For systems categorized as Moderate, or higher

a. Authorize the use of remote access for execution of privileged commands and access to security-relevant information only when there are compelling business needs; and
b. Document the rationale for such access in the system security plan.

AC-18 - Wireless Access (L, *O*)

For all systems

a. Establish usage restrictions, configuration / connection requirements, and implementation guidance for wireless access; and
   1. Wireless access on client machines that do have an essential business purpose for wireless access, must be configured to allow access only to authorized wireless networks, and to restrict access to other wireless networks; and (CIS-15.5); and
   2. Agency guest wireless networks must be fully segregated and independent of agency internal networks; and
b. Authorize wireless access to the system prior to allowing such connections.

NOTE: Wireless technologies include, for example, microwave, packet radio (ultra-high frequency/very-high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols that provide credential protection and mutual authentication.

AC-18(1) - Wireless Access | Authentication and Encryption (M, S)
For all systems

a. Protect wireless access to the system using user authentication and approved cryptographic protections (CIS-15.7); and

For systems categorized as Moderate, or higher

b. Protect wireless access to the system using device authentication protocols, such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which require mutual multifactor authentication (CIS-15.8).

AC-18(3) - Wireless Access | Disable Wireless Networking (M, O/S)
For systems categorized as Moderate, or higher

a. Disable, when not intended for use, wireless networking capabilities internally embedded within system components prior to issuance and deployment, including:
   1. Wireless access for devices that do not have a business purpose for wireless access (CIS-15.4);
   2. Peer-to-peer (ad-hoc) wireless network capabilities on wireless clients (CIS-15.6); and
   3. Peripheral wireless access of devices (such as Bluetooth and NFC), unless such access is required for a documented business purpose (CIS-15.9).

AC-19 - Access Control for Mobile Devices (L, *O*)

For all systems

a. Establish and document usage restrictions, configuration / connection requirements, and implementation guidance, for organization-controlled mobile devices;
b. Explicitly authorize the connection of mobile devices to organizational systems; and
c. Protect and control mobile devices using a mobile device management solution. Mobile devices must not be left unattended while outside of controlled areas.

NOTE: A mobile device is a computing device that:

1. Has a small form factor such that it can easily be carried by a single individual;
2. Is designed to operate without a physical connection (e.g. wirelessly transmit or receive information);
3. Possesses local, non-removable or removable data storage; and
4. Includes a self-contained power source.

AC-19(5) - Access Control for Mobile Devices | Full Device / Container-based Encryption (M, O)

For systems categorized as Moderate, or higher

Employ full-device encryption on all mobile devices to protect the confidentiality and integrity of information (CIS-13.6).

AC-20 - Use of External Systems (L, *O*)

For all systems

a. Establish terms and conditions, consistent with any 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.

NOTE: External systems are systems or components of systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. This includes systems managed by contractors, and systems owned by other agencies. This control addresses the use of external systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services from organizational systems.

AC-20(2) - Use of External Systems | Portable Storage Devices (M, O)

Enterprise wide

a. Document and approve the use of agency-controlled portable storage devices when used on external systems. Documentation must include:
   1. Device ID;
   2. Personnel authorized to use the portable storage device;
   3. Purpose for use; and
   4. Date range of use.

AC-20(3) - Use of External Systems | Non-Organizationally Owned Systems and Components (NS, O)

Enterprise wide

Provide an exception and approval process by which the agency grants and documents approval to attach portable devices (cameras, I-phones, USB drives, etc.) not owned by the agency, to agency owned equipment.

AC-22 - Publicly Accessible Content (L, *O*)

For all systems

a. Designate individuals that are authorized to post information onto a publicly accessible system;

b. Train authorized individuals to ensure that publicly accessible information does not contain non-public information, including information classified at Level 2 (Limited) or above according to the statewide Information Asset Classification Policy;
c. Review content after editing, and prior to posting onto the publicly accessible system to ensure that non-public information is not included; and
d. Review content on the publicly accessible system for non-public information, and remove such information if discovered. Personnel conducting these reviews shall be different from the personnel posting content, or conducting the reviews prior to posting content.

AWARENESS AND TRAINING – AT

AT-2 - Security Awareness Training (L, *O*)

Enterprise wide

a. Provide all personnel (including but not limited to managers, senior executive staff, contractors, and volunteers) basic security awareness training:
   1. As part of initial training for new personnel and before authorizing access to state systems, and information;
   2. When required by system changes; and
   3. At least annually thereafter; and
b. Create a security awareness program for all personnel to complete on a regular basis to ensure understanding of the necessary behaviors and skills to help support the security of the enterprise (CIS-17.3):
   1. The Security Awareness Program must be updated at least annually to address new technologies, threats, standards, and business requirements (CIS-17.4); and
   2. At a minimum, training must include:
      i) Information on enabling and using secure authentication (CIS-17.5);
      ii) Proper identification, storage, transfer, and destruction of sensitive information (CIS-17.7);
      iii) Identification of common indicators of an incident; and
      iv) How to report incidents (CIS-17.9);
c. All personnel with access to state information assets shall complete basic statewide security awareness training as required; and
d. Provide additional training, including any training required for access to regulated data to supplement the statewide mandated awareness training.

AT-2(2) - Security Awareness Training | Insider Threat (M, O)

Enterprise wide

Include security awareness training that covers the recognition and reporting of potential indicators of insider threat, including unintentional data exposure (e.g. loss of mobile devices, sending an email to the wrong recipient, etc.) (CIS-17.8).

AT-2(3) - Security Awareness Training | Social Engineering and Data Mining (M, O)

Enterprise wide

Include security awareness training that covers the recognition and reporting of potential and actual instances of social engineering and social mining (e.g. phishing, phone scams, impersonation, etc.) (CIS-17.6).

AT-3 - Role-Based Training (L, *O*)

Enterprise wide

a. Provide role-based security-related training to personnel with the following roles and responsibilities:
   1. Software development personnel in secure coding practices for their specific development environment and responsibilities (CIS-18.6);

    2. Personnel with privileged access; and
    3. Other personnel as required by applicable laws, executive orders, directives, policies, regulations, standards, and guidance; and

b. Provide role-based security-related training:
    1. As part of initial training for new users and before authorizing access to organization systems, information, and regulated data;
    2. When required by system changes; and
    3. At least annually thereafter.

AT-4 - Security Training Records (L*, O*)

Enterprise wide

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

b. Retain individual training records according to applicable laws, executive orders, directives, policies, regulations, standards, and guidance, but in no case less than the retention time specified by the Oregon Secretary of State Archive Division.

AUDIT AND ACCOUNTABILITY – AU

AU-2 - Audit Events (L, *O*)

Enterprise wide

a. Verify that, at a minimum, all systems are capable of auditing the following events:
   1. Startup and shutdown;
   2. Installation and removal of software;
   3. Error messages;
   4. Account creation, modification, or deletion;
      i) Systems must be configured to issue an alert when an account is added to or removed from any group assigned administrative privileges (CIS-4.8);
   5. User logon and logoff;
   6. Unsuccessful logon attempts (CIS-4.9);
   7. Attempted access to deactivated accounts (CIS-16.12);
   8. Successful and unsuccessful change of password;
   9. Creation or modification of super-user groups; (CIS-4.8)
   10. Startup and shutdown of audit functions;
   11. Manual clearing or modification of the audit log file;
   12. Change of file or user permissions or privileges (e.g. use of SUID/GUID, CHOWN, SU, etc.);
   13. Execution of command-line processes for command shells such as Microsoft PowerShell and Bash (CIS-8.8);
   14. Changes made to an application or database by a batch file;
   15. Changes to database or application records, where the application has been bypassed to produce the change (via file or other database utility);
   16. Modifications to the application or database;
   17. Accesses to information and files;
   18. Configuration changes;
   19. Remote access outside of the internal network, and all dial-in access to the system;
   20. Domain Name System (DNS) query logging for detection of hostname lookups for known malicious domains (CIS-8.7);
   21. Execution of command-line processes for command shells such as Microsoft PowerShell and Bash (CIS-8.8);
   22. Remote access outside of the internal network, and all dial-in access to the system;
       NOTE: Remote access is defined as a type of network access that involves communication through external networks. Internal networks include LANs and WANs; and
   23. All system and interactions concerning:
       i) Information classified as Level 3 (Restricted) or above according to the statewide Information Asset Classification Policy; and

b. Coordinate the security audit function with other organizational entities requiring audit-related information, to enhance mutual support and help guide the selection of auditable events; and

c. Document a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

AU-2(3) - Audit Events | Review and Update (M, O)

For systems categorized as Moderate, or higher

Review and update audited events at least annually, or when a major change to the system occurs.

AU-3 - Content of Audit Records (L, *S*)

For all systems

a. Configure systems to generate audit records containing sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. At a minimum, the following elements shall be identified within each audit record (CIS-6.3):

1. Date and time when the event occurred;
2. The software or hardware component of the system where the event occurred;
3. Source of the event (e.g. network address, console);
4. Type of event that occurred;
5. Subject identity (e.g. user, device, process context);
6. The outcome (i.e. success or failure) of the event; and
7. Network traffic data on all network boundary devices (CIS-12.8).

AU-3(1) - Content of Audit Records (M, S)
For systems categorized as Moderate, or higher

Generate audit records containing additional information as required by applicable laws and regulations, specific to the system.

AU-4 - Audit Storage Capacity (L*, O/S*)

For all systems

Allocate sufficient audit record storage capacity to comply with State of Oregon records retention schedules and any other applicable retention requirements (CIS-6.4).

AU-5 - Response to Audit Processing Failures (L*, S*)

For all systems

a. Configure to provide alerts to designated Agency personnel in the event of audit processing failures when the failure occurs;
b. Take appropriate action to address the restoration of logging functionality immediately upon discovery; and
c. Ensure that systems receiving, processing, or storing regulated data comply with applicable laws and regulations, specific to the system.

AU-5(1) - Response to Audit Processing Failures | Audit Storage Capacity (H, S)
For systems categorized as Moderate, or higher

Provide a warning to designated officials (to include system administrators, Information Security Officers, Operational Security Officers) when allocated audit record storage volume reaches 80% utilization, or as specified by regulations specific to the system.

AU-6 - Audit Review, Analysis, and Reporting (L*, O*)

For all systems

a. Review and analyze system audit records at least weekly for the following:
   1. Indications of inappropriate or unusual activity related to potential unauthorized access (CIS-6.7); and
   2. Other anomalies or abnormal events;
b. Report incidents discovered during audit record review and analysis according to agency, State of Oregon, and Federal Incident Response Policy and procedures.
   1. Findings involving a potential unauthorized disclosure of FTI must be reported to the office of the appropriate special agent-in-charge for the Treasury Inspector General for Tax Administration (TIGTA) and to the IRS Office of Safeguards immediately, but no later than 24 hours after identification of the possible incident; and
   2. Findings involving a potential unauthorized disclosure of Social Security Administration Provided Information (SSPI) must be reported to the Social Security Administration Regional Office or System Security Contact within one hour after identification of the possible incident.

AU-6(1) - Audit Review, Analysis, and Reporting | Process Integration (M, O)
For systems categorized as Moderate, or higher

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

AU-6(3) - Audit Review, Analysis, and Reporting | Correlate Audit Repositories (M, O)
For systems categorized as Moderate, or higher

Analyze and correlate audit records across different repositories to gain Agency-wide situational awareness (CIS-6.5).

AU-6(4) - Audit Review, Analysis, and Reporting | Central Review and Analysis (M, S)
For systems categorized as Moderate, or higher

a. Aggregate logs to a central log management system for analysis and review. Automated mechanisms for centralized reviews and analyses include, for example, Security Information and Event Management (SIEM) products (CIS-6.6); and
b. Send malware detection events to anti-malware administration tools and centralized log servers for alerting and analysis (CIS-8.6).

AU-7 - Audit Reduction and Report Generation (M*, S*)

For systems categorized as Moderate, or higher

a. Provide and implement an audit reduction and report generation capability that:
   1. Supports near real-time audit review, analysis, and reporting requirements described in AU-6, and after-the-fact investigations of security incidents;
      i) The audit reduction and report capability must be tuned on a regular basis in order to better identify actionable events and decrease event noise (CIS-6.8); and
   2. Does not alter the original content or time ordering of audit records.

AU-7(1) - Audit Reduction and Report Generation | Automatic Processing (M, S)
For systems categorized as Moderate, or higher

Provide and implement the capability to process audit records for events of interest based on individual items, or combinations of items contained in the audit records, as defined in AU-3 (CIS-6.8).

AU-8 - Time Stamps (L*, S*)

For all systems

a. Use internal system clocks to generate time stamps for audit records.
   1. Time stamps generated by the systems shall include both the date and the time; and
b. Record time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) (CIS-6.1).

AU-8(1) - Time Stamps | Synchronization With Authoritative Time Source (M, S)
For all systems

a. Provide at least two authoritative State of Oregon time sources for synchronization;
b. The State authoritative time sources must be sourced by at least three unique Stratum One time sources;
c. Compare and synchronize internal system clocks with at least one of the Oregon enterprise-wide primary authoritative time sources, to ensure that time stamps in audit records are as accurate as possible and correlate across different systems or system components (CIS-6.1); and
d. Configure internal system clocks to synchronize to the authoritative time source at least weekly, or when the time difference between systems is greater than 5 minutes.

AU-8(2) - Time Stamps | Secondary Authoritative Time Source (NS, S)
For all systems

   a. Identify a secondary Oregon enterprise-wide authoritative time source that is in a different geographic region than the primary authoritative time source; and
   b. Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.

AU-9 - Protection of Audit Information (L, *S*)

For all systems

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

AU-9(4) - Protection of Audit Information | Access by Subset of Privileged Users (M, O)

For systems categorized as Moderate, or higher

Limit access to management of audit functionality to personnel that have a need to know and have been expressly authorized for this function.

AU-9(6) - Protection of Audit Information | Read Only Access (M, O/S)

For systems categorized as Moderate, or higher

Ensure audit files are tamper resistant (read-only). In all cases, access to the logs must be limited only to those with a need to access.

AU-11 - Audit Record Retention (L, O)

For all systems

a. Retain audit records, as defined under AU-2, to provide support for after-the-fact investigations of IT security incidents; and
b. Retain all audit records in accordance with Oregon Administrative Rule 166-300-0030 (3) for Computer System Security Records and applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance, whichever is most restrictive.

AU-12 - Audit Generation (L, *S*)

For all systems

a. Provide audit record generation capability for the list of auditable events defined under AU-2 a., with content prescribed under AU-3 on, at a minimum, the following system components (CIS-6.2):
   1. Hardware or devices:
      i) Network devices (e.g. switches, routers, firewalls);
      ii) Workstations;
      iii) Servers;
      iv) Cameras;
      v) Printers;
      vi) Multi-function devices;
      vii) Industrial controls;
      viii) Other devices with wired or wireless connectivity (e.g. Internet of Things devices); and
      ix) Mobile devices (excluding Limited Feature Devices); and
   2. Software:
      i) Operating systems (excluding “limited feature” operating systems);
      ii) Applications;
      iii) Databases; and
      iv) Firmware;
b. Limited-Feature Operating Systems: Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g. Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). Limited-feature operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network

based technical attacks due to the limited feature sets. Devices using these operating systems are required to be managed by a mobile device management solution; and

c. Agency System Owners, Agency Information Owners, Systems Auditors, and Business Information Security Officers, shall be allowed to select which auditable events are applicable to be audited by specific components of their respective systems.

AU-16 - Cross-Organizational Auditing (NS*, O*)

For systems categorized as Moderate, or higher

When agencies use systems and/or services of external organizations, employ mechanisms for coordinating the access and protection of audit information when transmitting across agency boundaries. The external organization or third-party service provider must be held accountable to protect and share audit information with the agency by contract.

SECURITY ASSESSMENT AND AUTHORIZATION (CA)

CA-2 - Security Assessments (L, *O*)

For all systems

a. Assess controls at the initiation, and throughout all phases of the system development life cycle process;
b. Develop a security assessment plan that describes the scope of the assessment, including:
   1. The security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine control effectiveness; and
   3. The assessment environment, assessment team, and assessment roles and responsibilities;
c. Ensure the assessment plan is reviewed and approved by the authorizing official, or designated representative, prior to conducting the assessment;
d. Assess the security controls in the system and its environment, at a minimum, on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
e. Produce a security assessment report that documents the results of the assessment; and
f. Provide the results of the security control assessment to the authorizing official and other parties as described in the Oregon Statewide Security Plan.

CA-2(1) - Security Assessments | Independent Assessors (M, O)

For systems categorized as Moderate, or higher

Employ independent assessors or assessment teams to conduct security control assessments.

NOTE: Independent assessors or assessment teams are individuals or groups conducting impartial assessments of systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness.

CA-2(2) - Security Assessments | Specialized Assessments (H, O)

For all systems

Include, as part of security control assessments, regular scans from outside each trusted network boundary to detect any unauthorized and open ports that are accessible across the boundary (CIS-12.2).

CA-3 - System Interconnections (L, *O*)

For all systems

a. Authorize connections from the system to other systems using Interconnection Security Agreements;
b. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Review and update Interconnection Security Agreements on an annual basis.

NOTE: This control applies to dedicated connections between two or more separate systems and does not apply to transitory, user-controlled connections such as email and website browsing. The System Security Plan is an appropriate place to document the existence of interconnection security agreements associated with the system.

CA-3(5) - System Interconnections | Restrictions on External System Connections (M, O)

For systems categorized as Moderate, or higher

Employ a deny-all, permit-by-exception methodology for allowing systems to connect to external systems.

CA-5 - Plan of Action and Milestones (L, *O*)

For all systems

a. Develop a plan of action and milestones for systems, to document the planned remedial actions of the organization to correct weaknesses or deficiencies noted during the assessment of security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Update existing plan of action and milestones on a continual basis, and review quarterly, based on the findings from control assessments, impact analyses, continuous monitoring activities, vulnerability assessments, penetration testing, and remediation actions.

CA-6 - Security Authorization (L*, O*)

For all systems

a. Assign a senior-level executive or manager as the Authorizing Official for the system and for any common controls inherited by the system;
b. Ensure that the Authorizing Official, before commencing operations:
   1. Authorizes the system for processing; and
   2. Authorizes the common controls inherited by the system; and
c. Document the authorizations in the System Security Plan. Authorizations must be updated every three years, or any time there is a significant change to the system.

CA-7 - Continuous Monitoring (L*, O*)

For all systems

a. Develop and implement a continuous security monitoring strategy, and programs that include:
   1. Establishing the security metrics to be monitored, and documented in the applicable System Security Plan;
   2. Establishing continuous monitoring and annual assessments of security control effectiveness;
   3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
   4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
   5. Correlation and analysis of security-related information generated by security control assessments and monitoring;
   6. Response actions to address results of the analysis of security-related information; and
   7. Reporting the security status of the organization and organizational systems to the Agency Director, or designee thereof, at the frequency defined in the agency's continuous security monitoring strategy.

CA-7(1) - Independent Assessments (M, O) .

For systems categorized as Moderate, or higher

Employ independent assessors or assessment teams to monitor the security and privacy controls in the system on an ongoing basis.

CA-7(4) - Risk Monitoring (L)

For all systems

a. Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:
   1. Effectiveness monitoring;
   2. Compliance monitoring; and
   3. Change monitoring.

NOTE: Effectiveness monitoring determines the ongoing effectiveness of implemented risk response measures. Compliance monitoring verifies that the required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

CA-8 - Penetration Testing (H*, O*)

For systems classified as Moderate, or higher

a. Establish and execute a program for penetration tests that includes a full scope of blended attacks, including, but not limited to: wireless, client-based, and web application attacks (CIS-20.1).
   1. Conduct and document penetration testing at least annually;
   2. Include external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully (CIS-20.2);
   3. Include tests looking for the presence of unprotected system information and artifacts that would be useful to attackers. Such information might include: network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords, or other information critical to system operation (CIS-20.4);
   4. For elements that are not typically tested in production, such as attacks against Supervisory Control and Data Acquisition and other controls, a test bed that mimics the production environment must be set up and used for penetration tests and red team exercises when possible (CIS-20.5);
   5. Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments are to be used as a starting point to guide and focus penetration testing (CIS-20.6); and
   6. Control and monitor any user or system accounts used to perform penetration testing, to ensure that they are only being used for legitimate purposes. Such accounts must be removed or restored to normal function as soon as testing is finished (CIS-20.8).

CA-8(1) - Penetration Testing | Independent Penetration Agent or Team (H, O)

For systems classified as Moderate +

Employ an independent third-party penetration agent or penetration team to perform penetration testing on the system or system components. Independent, third-party penetration tests must be conducted at least every three years.

CA-8(2) - Penetration Testing | Red Team Exercises (NS, O)

For systems classified as Moderate +

a. Perform annual red team exercises to test statewide readiness to identify, respond to, and stop attacks (CIS-20.3); and
b. Document red team test results using open, machine-readable standards (e.g. SCAP), and must be scored and compared over time (CIS-20.7).

CA-8(3) - Penetration Testing | Facility Penetration Testing (NS, O)

For areas containing systems classified as Moderate, or higher

a. Employ a penetration testing process that includes attempts to bypass or circumvent controls associated with physical access points to the facility.
   1. Announced facility penetration testing must be conducted at least quarterly; and
   2. Unannounced facility penetration must be conducted at least annually.

CA-9 - Internal System Connections (L*, O*)

For all systems

a. Authorize internal connections of intra-system components to the system; and
b. For each intra-system connection, document, via the System Security Plan for the system: the internal connections; interface characteristics; security requirements; and the nature of the information communicated.

NOTE: This control applies to connections between organizational systems and separate constituent system components. These intra-system connections include, for example, system connections with mobile devices, notebook computers, desktop computers, workstations, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal system connection, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations. This can include, for example, all digital printers, scanners, and copiers with a specified processing, transmission, and storage capability or all smart phones with a specific baseline configuration.

CONFIGURATION MANAGEMENT (CM)

CM-2 - Baseline Configuration (L*, O*)

For all systems

a. Develop, document, and maintain current baseline configurations;
b. Review and update the baseline configurations:
   1. At a minimum, annually;
   2. When required due to system upgrades, patches, or other significant changes;
   3. As an integral part of system component installations and upgrades;
   4. All network device configurations must be compared against approved security configurations defined for each network device in use; and (CIS-11.3); and
   5. Agency System Owners alerted when deviations are discovered (CIS-11.3); and
c. Document the baseline configuration, and provide information about the components of a system, including:
   1. Security configurations for all authorized operating systems and software (CIS-5.1);
   2. Security configurations for all authorized network devices (CIS-11.1); and
   3. Hardening configurations for databases (CIS-18.11).

CM-2(2) - Baseline Configuration | Automation Support for Accuracy and Currency (M, O)

For systems categorized as Moderate, or higher

Employ automated mechanisms / configuration management tools that will enforce and redeploy configuration settings to systems at regularly scheduled intervals so as to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the system (CIS-5.4).

CM-2(3) - Baseline Configuration | Retention of Previous Configurations (M, O)

For systems categorized as Moderate, or higher

Retain secure images or templates, according to approved configuration standards, for all systems in the enterprise. Any new system deployments must use one of the approved images or templates (CIS-5.2).

CM-2(7) - Baseline Configuration | Configure Systems and Components For High-Risk Areas (M, O)

For systems categorized as Moderate, or higher

a. When equipment will be used during international travel:
   1. Issue laptops or other portable computing devices with no access to state networks;
   2. No VPN access to state networks;
   3. WebMail access is allowed; and
   4. For systems that contain data classified as level 3 or above, the system cannot contain restricted data other than that which is necessary for the purpose associated with the travel; and
b. Upon return from international travel:
   1. Do not connect systems to internal networks;
   2. Copy data to external media and scan before transferring data to state network devices; and
   3. Re-image systems before connecting to the state network.

CM-3 - Configuration Change Control (M*, O*)

For systems categorized as Moderate, or higher

a. Determine the types of changes to systems that are to be configuration-controlled;
b. Utilize a change control management process to review proposed configuration-controlled changes to the systems, and document approval or denial of such changes with explicit consideration for security impact analysis;
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 systems according to applicable laws, executive orders, directives, policies, regulations, standards, and guidance;
f. Monitor and review activities associated with configuration-controlled changes to the system;
g. Coordinate and provide oversight for configuration change control activities through regular change control meetings.
   1. The frequency of these meetings is dependent upon the needs of the agency, and should take into account the typical number and impact of changes; and
h. Include changes to components of the system, and changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers); and
i. Establish and follow procedures to approve attachment of peripheral devices to workstations and servers. Only approved devices may be attached.

CM-3(2) - Configuration Change Control | Test / Validate / Document Changes (M, O)

For systems categorized as Moderate, or higher

Test, validate, and document changes to the system before fully implementing the changes on the system.

CM-3(4) - Configuration Change Control | Security Representative (M, O)

For systems categorized as Moderate, or higher

Require security representation as a part of the change advisory board or process.

CM-4 - Security and Privacy Impact Analysis (L*, O*)

For all systems

Analyze changes to systems to determine potential security impacts prior to change implementation.

CM-4(2) - Security and Privacy Impact Analysis | Verification of Security and Privacy Functions (M, O)

For systems categorized as Moderate, or higher

Verify security and privacy functions after system changes, to ensure that the functions 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 (L*, O*)

For all systems

a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system;
b. Access restrictions for change also include software libraries; and
c. Store baseline images and templates on secure servers, and validate with integrity monitoring tools, to ensure that only authorized changes to the images are possible (CIS-5.3).

CM-6 - Configuration Settings (L*, O*)

For all systems

a. Establish and document a standard set of mandatory configuration settings for information technology products employed within the system, and reflect the most restrictive mode consistent with operational requirements (CIS-5.1);
b. At a minimum, agencies must meet the CIS Benchmark Level 1 configuration guidelines for any new or any updates to existing software, hardware, or device;
c. Implement the configuration settings;
d. Identify, document, and approve exceptions from mandatory configuration settings for components within the system based on operational requirements; and
e. Monitor and control changes to the configuration settings, in accordance with applicable federal, state, and agency regulations, policies, and procedures.

CM-7 - Least Functionality (L, *O*)

For all systems

a. Configure the system to provide only essential capabilities (CIS-5.1);
b. Disable by default, all network ports, protocols, server roles, and services;
c. Permit only network ports, protocols, server roles, and services for which there is a validated and documented business need (CIS-9.2);
d. Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities (CIS-14.2);
e. Disable all workstation-to-workstation communication, to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or micro-segmentation (CIS-14.3); and
f. Protect all information stored on file systems, network shares, claims, applications, and databases using specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities (CIS-14.6).

CM-7(1) - Least Functionality | Periodic Review (L, O)

For all systems

a. Review systems at least annually to identify unnecessary and / or non-secure functions, ports, protocols, and services. Automated port scans must be performed at least monthly against all systems, and alert if unauthorized ports are detected on a system; and (CIS-9.3); and
b. Disable unnecessary functions, ports, protocols, and/or services.

CM-7(5) - Least Functionality | Authorized Software / Whitelisting (M, O)

For systems categorized as Moderate, or higher

a. Identify and maintain a current inventory all software assets that are authorized to execute on the system;
b. Employ a deny-all, permit-by-exception methodology to allow the execution of authorized software programs on the system;
c. The Agency must utilize application whitelisting technology on all information assets to ensure that only authorized software executes and all unauthorized software is blocked from execution (CIS-2.7);
   1. The Agency's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process (CIS-2.8); and
   2. The Agency's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system (CIS-2.9); and
d. Review and update the list of authorized software programs, in order to ensure that unauthorized software is either removed, or the inventory is updated in a timely manner (CIS-2.6):
   1. At a minimum quarterly;
   2. When required due to system upgrades or other significant changes; and
   3. As an integral part of system component installations.

CM-8 - System Component Inventory (L, *O*)

For all systems

a. Develop and document an inventory of system components that:
   1. Accurately reflects the current system;
   2. Includes all components within the authorization boundary of the system; and
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
b. The hardware asset inventory must include any information determined to be necessary by the Agency to achieve effective property accountability, including but not limited to (CIS-1.5):
   1. The network addresses;
   2. Machine name;

3. Type;
4. Model;
5. Serial Number;
6. System / component owner;
7. Department for each asset;
8. Whether the hardware asset has been approved to connect to the network; and
9. Any active ports, protocols, and services associated with listed hardware assets (CIS-9.1);

c. Review and update the system component inventory at least annually;
d. Utilize an active discovery tool to identify devices within the system boundary, and update the system component inventory (CIS-1.1); and
e. Utilize a passive discovery tool to identify devices within the system boundary, and automatically update the system component inventory (CIS-1.2).

CM-8(1) - System Component Inventory | Updates During Installation / Removals (M, O)
For systems categorized as Moderate, or higher

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

CM-8(3) - System Component Inventory | Automated Unauthorized Component Detection (M, O)
For systems categorized as Moderate, or higher

a. Employ automated mechanisms at least weekly to detect the presence of unauthorized hardware, software, and firmware components within the system;
   1. Network vulnerability scanning tools must be configured to detect and alert on unauthorized wireless access points connected to the organization’s wired network (CIS-15.2); and
b. When detected, remove or quarantine unauthorized components from the network (CIS-1.6).

CM-9 - Configuration Management Plan (M)

For systems categorized as Moderate, or higher

Develop, document, and implement a configuration management plan for systems, 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 the Agency Chief Information Officer (CIO) or equivalent, or designee thereof; and
e. Protects the configuration management plan from unauthorized disclosure and modification.

CM-10 - Software Usage Restrictions (L, *O*)

For all systems

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 technologies to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

NOTE: Attackers continuously scan organization for vulnerable versions of software that can be exploited. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets.

CM-10(1) - Software Usage Restrictions (NS, O)
For systems categorized as Moderate, or higher

Establish restrictions on the use of open source software. Open source software must:

a. Be legally licensed;
b. Be approved by the Agency CIO or designee; and
c. Adhere to a secure configuration baseline from the U.S. Government or an accepted industry standard.

CM-11 - User-Installed Software (L*, O*)

For all systems

Prohibit users from downloading, installing, or otherwise using unauthorized software on Agency-owned systems.

CM-12 - Information Location (M*, O*)

For systems categorized as Moderate, or higher

a. Maintain an inventory of the types of sensitive (Level 3 or greater) information stored, processed, or transmitted by the organization's technology systems, including that which is located onsite or at a remote service provider. Identify the location of and the specific system components on which the sensitive information resides (CIS-13.1);
b. Identify and document users who have access to the system and system components where sensitive information resides; and
c. Document changes to the location (i.e., system or system components) where sensitive information resides.

CM-12(1) - Information Location | Automated Tools to Support Information Location (M, O)

For systems categorized as Moderate, or higher

Use automated active discovery tools to identify sensitive (Level 3 or greater) information that is stored, processed, or transmitted by state agency technology systems, including that which is located onsite or at a remote service provider, and update the organization’s sensitive information inventory (CIS-14.5).

CONTINGENCY PLANNING (CP)

CP-2 - Contingency Plan (L, *O*)

For all systems

a. Develop a contingency plan for the system(s) that:
   1. Identifies essential missions and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, to include contact information for individuals with assigned responsibilities;
      i) The plan shall include a detailed contact list. At a minimum, the contact list shall include primary (office) and secondary telephone numbers. The contact list shall also describe the contact escalation process. The contact list shall also be updated out-of-cycle to address changes to Contingency Plan personnel;
   4. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;
   5. Addresses eventual, full system restoration without deterioration of the security and privacy controls originally planned and implemented; and
   6. Is reviewed and approved by the Agency Head;

b. Distribute copies of the contingency plan to key contingency personnel;
   1. Agencies must notify key contingency personnel of changes to the contingency plan, and make updated copies of the contingency plan available to them;

c. Coordinate contingency planning activities with incident handling activities to ensure that the necessary planning activities are in place and activated in the event of a security incident;

d. Review the contingency plan for the system at least annually;

e. Update the contingency plan to address changes to the Agency, system, or operational environment as they occur;

f. Update the contingency plan to address problems encountered during contingency plan implementation, execution, or testing; and

g. Protect the contingency plan from unauthorized modification and disclosure.

CP-2(1) - Contingency Plan | Coordinate With Related Plans (M, O)

For systems categorized as Moderate, or higher

Coordinate the development of contingency plans with the development of related plans (e.g. Business Continuity, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans and Occupant Emergency Plans).

CP-2(3) - Contingency Plan | Resume Essential Missions / Business Functions (M, O)

For systems categorized as Moderate, or higher

a. Within the Contingency Plan and Business Impact Analysis, define the time period(s) in which systems must be operational to support essential mission and business functions by:
   1. Working with mission / business process owners, section personnel, managers, and other stakeholders, the following three downtime factors must be considered relative to a disruptive event:
      i) Maximum Tolerable Downtime (MTD): The maximum amount of time that mission / business processes can be disrupted without causing harm to the organization's mission;
      ii) Recovery Time Objective (RTO): the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and supported mission/business processes; and
      iii) Recovery Point Objective (RPO): The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part

of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process;

2. Planning for the resumption of operation to be within the defined time period in which systems needs to be operational after activating the contingency plan; and
3. Ensuring that system assets supporting essential mission and business functions are identified and included in the organization-wide contingency plan.

CP-2(8) - Contingency Plan | Identify Critical Assets (M, O)
For systems categorized as Moderate, or higher

Identify and document critical system assets supporting essential mission and business functions.

NOTE: Critical system assets include both technical and operational aspects. Technical aspects include, for example, information technology services, system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can aid in identifying critical assets.

CP-3 - Contingency Training (L*, O*)

For all systems

Provide contingency training to system users consistent with their assigned contingency roles and responsibilities:

a. Prior to being assuming a contingency role or responsibility;
b. Any time the system undergoes a significant change; and
c. Annually thereafter.

CP-4 - Contingency Plan Testing (L*, O*)

For all systems

a. Test the contingency plan, at a minimum annually, to determine the effectiveness of the plan and the agency’s readiness to execute the plan;
b. Document and review contingency plan test results; and
c. Document and initiate corrective actions as needed.

CP-4(1) - Contingency Plan | Coordinate With Related Plans (M, O)
For systems categorized as Moderate, or higher

Coordinate Contingency Plan testing with agency areas or organizational units charged with responsibility for related plans.

CP-6 - Alternate Storage Site (M*, O*)

For systems categorized as Moderate, or higher

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 security controls equivalent to that of the primary site.

CP-6(1) - Alternate Storage Site | Separation from Primary Site (M, O)
For systems categorized as Moderate, or higher

Identify an alternate storage site that is geographically separated from the primary storage site to reduce susceptibility to the same threats.

CP-6(3) - Alternate Storage Site | Accessibility (M, O)
For systems categorized as Moderate, or higher

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

NOTE: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

CP-7 - Alternate Processing Site (M*, O*)

For systems categorized as Moderate, or higher

a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of system operations for essential missions and business functions within time-periods consistent with agency-defined recovery time and recovery point objectives;
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 agency-defined time-period for transfer and resumption; and
c. Provide information security safeguards at the alternate processing site that are equivalent to those at the primary site.

CP-7(1) - Alternate Processing Site | Separation from Primary Site (M, O)

For systems categorized as Moderate, or higher

Identify an alternate processing site that is geographically separated from the primary processing site to reduce susceptibility to the same threats.

CP-7(2) - Alternate Processing Site | Accessibility (M, O)

For systems categorized as Moderate, or higher

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

NOTE: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

CP-7(3) - Alternate Processing Site | Priority of Service (moderate, O)

For systems categorized as Moderate, or higher

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with agency-defined recovery time and recovery point objectives.

CP-8 - Telecommunications Service (M*, O*)

For systems categorized as Moderate, or higher

Establish alternate telecommunications services including necessary agreements to permit the resumption of system operations for essential missions and business functions within agency-defined recovery time and recovery point objectives.

NOTE: This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites.

CP-8(1) - Telecommunications Service | Priority of Service Provisions (M, O)

For systems categorized as Moderate, or higher

a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements, including agency-defined recovery time and recovery point 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(2) - Telecommunications Service | Single Points of Failure (M, O)

For systems categorized as Moderate, or higher

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

CP-9 - System Backup (L, *O*)

For all systems

a. Conduct backups of user-level information contained in the system according to agency-defined frequency, recovery time, and recovery point objectives (CIS-10.1);
b. Conduct backups of system-level information contained in the system according to agency-defined frequency, recovery time, and recovery point objectives. System-level information includes, for example, system state, operating system and application software, and licenses (CIS-10.1);
c. Conduct backups of system documentation, including security-related documentation, according to the agency-defined frequency, recovery time, and recovery point objectives (CIS-10.1); and
d. Protect the confidentiality and integrity of the system backup information according to applicable protection standards and disclosure provisions relative to the system level categorization and regulated data requirements.

CP-9(1) - System Backup | Testing for Reliability / Integrity (M, O)

For all systems

a. Test backup information at least annually for media reliability and information integrity (CIS-10.3);
   1. Testing may be conducted on random files as opposed to entire system restoration; and
   2. Test results must be documented and include findings for media reliability and information integrity; and
b. As part of contingency plan testing, use a sample of backup information to restore selected system functions. This may be a full restoration, or a restoration of selected files.

CP-9(8) - System Backup | Cryptographic Protection (M, O)

For all systems

Encrypt backup information in order to protect the confidentiality and integrity of the information (CIS-10.4).

CP-10 - System Recovery and Reconstruction (L, *O*)

For all systems

a. Provide for the recovery and reconstitution of the system to a known state after a disruption, compromise, or failure within agency-defined recovery time and recovery point objectives; and
b. Ensure that critical system assets supporting essential missions and business functions are backed up, through a process such as imaging, to provide for the recovery and reconstruction of the system to a known good state after a disruption, compromise, or failure (CIS-10.2).

CP-10(2) - System Recovery and Reconstruction (M, O)

For systems categorized as Moderate, or higher

Implement transaction recovery for systems that are transaction-based.

IDENTIFICATION AND AUTHENTICATION (IA)

IA-2 - Identification and Authentication (L*, O/S*)

For all systems

Uniquely identify and authenticate users, or processes acting on behalf of users.

IA-2(1) - Identification and Authentication | Multifactor Authentication to Privileged Accounts (L, S)
For all systems

Implement multifactor authentication for access to privileged accounts (CIS-4.5) (CIS 11.5).

IA-2(2) - Identification and Authentication | Multifactor Authentication to Non-Privileged Accounts (L, S)

For all systems

a. Implement multifactor authentication for access to non-privileged accounts; and

For systems categorized as Moderate, or higher

b. Tie multifactor authentication to an individual.

NOTE: When user-based certificates are used for multifactor authentication purposes, they must:

1. Specify an individual user and not a particular device;
2. Prohibit multiple users from utilizing the same certificate; and
3. Require the user to “activate” that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

IA-2(8) - Identification and Authentication | Access to Accounts – Replay Resistant (L, S)
For all systems

Implement replay-resistant authentication mechanisms for access to privileged accounts.

NOTE: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.

IA-3 - Device-Level Identification and Authentication (M*, S*)

For systems categorized as Moderate, or higher

a. Configure systems to uniquely identify and authenticate end user-operated devices (e.g., workstations, laptops, voice-over-Internet Protocol (VoIP) phones, cell phones) and servers before establishing a connection to an internal network; and
b. Use only approved procedures, mechanisms, or protocols for host or device authentication. Approved mechanisms and protocols are:
   1. Port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network (CIS-1.7);
   2. Client certificates to authenticate hardware assets connecting to the organization's trusted network (CIS-1.8);
   3. Media Access Control (MAC) for device identification; and
   4. Other OSCIO approved organizational authentication solutions.

IA-4 - Identifier Management (L*, O*)

For all systems

Manage system identifiers by:

a. Receiving authorization from the documented Agency designated approving authority to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group role, or device; and
d. Preventing reuse of identifiers.

IA-5 - Authenticator Management (L, *O*)

For all systems

a. Verify the identity of the individual, group, role, or device receiving a system authenticator as part of the initial authenticator distribution.
b. Establish and define unique initial authenticator content for system authenticators in agency policy (CIS-4.2);
c. Ensure that authenticators for individuals, groups, roles, or devices have sufficient strength of mechanism for their intended use; and
d. Ensure that authenticators for shared group/role accounts are changed when membership to those accounts changes.

IA-5(1) - Authenticator Management | Password-Based Authentication (L, O/S)
For all systems

a. Enforce the following for password construction:
   1. Minimum length of ten (10) characters;
   2. At least one (1) numeric (e.g. zero – 9) and one (1) non-alphanumeric character (e.g. @, #, $, %, ^, &, etc.);
   3. At least one (1) English uppercase letter (e.g. A – Z);
   4. At least one (1) English lowercase letter (e.g. a – z);
   5. No dictionary words or common names; and
   6. No portions of the associated account name / identifier (e.g. User I.D., login name).

b. Enforce the following for password administration:
   1. Minimum lifetime of one (1) day;
   2. Maximum lifetime of 90 days;
   3. Change a password immediately in the event of a suspected compromise of the password or system; and
   4. Configure accounts with a history of at least 24 passwords, so a user cannot quickly re-use a previous password.
c. Store passwords using an OSCIO-approved hash algorithm and salt (CIS-16.4); and
d. Encrypt account user names and passwords during transmission (CIS-4.5) (CIS-16.5).

For systems not bound by federal regulatory requirements (e.g. IRS Publication 1075, CJIS, SSPI, PCI DSS, etc.), or where federal regulatory requirements allow, the following alternative password-based authentication standards may be used:

a. Enforce the following for password construction:
   1. Minimum length of fifteen (15) characters;
   2. Maximum length of up to sixty-four (64) characters;
   3. Acceptable characters include:
      Single Spaces
      All printable ASCII characters (RFC 20)
      All Unicode characters (ISO/IEC 10646)

b. Enforce the following for password administration:
   1. No maximum lifetime;

2. Change a password immediately in the event of a suspected compromise of the password or system;
3. Configure accounts with a history of at least 24 passwords, so a user cannot quickly re-use a previous password; and
4. Users shall have the option of using an OSCIO-approved password manager.

c. Store passwords using an OSCIO-approved hash algorithm and salt (CIS-16.4); and
d. Encrypt account user names and passwords during transmission (CIS-4.5) (CIS-16.5).

IA-5(5) - Authenticator Management | Change Authenticators Prior to Delivery (L, O)
For all systems

Change default authenticators to have values consistent with administrative level accounts prior to installation and deployment of the system (CIS-4.2).

IA-6 - Authenticator Feedback (L*, S*)

For all systems

Obscure authentication information (e.g., password, passphrase, PIN) during the authentication process to protect the information from possible exploitation or use by unauthorized individuals.

IA-7 - Cryptographic Module Authentication (L*, S*)

For all systems

Implement mechanisms for authentication to a cryptographic module that will meet the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.

IA-8 - Identification and Authentication (Non-Organizational Users) (L*, S*)

For all systems

a. Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users; and
b. Apply all supplemental controls identified under IA-2 (i.e., IA-2(1), IA-2(2), and IA-2(8)) to the identification and authentication of non-organizational users.

IA-11 - Identification and Authentication | Re-Authentication (L*, O, S*)

For all systems

a. Require users to re-authenticate within 7 days; and

For systems categorized as Moderate or higher

b. Require users to re-authenticate within 24 hours.

IA-12 - Identity Proofing (M*, O*)

Enterprise wide

a. Identity proof users that require accounts for logical access to systems. Identity proofing must be commensurate with the security categorization of the system;
b. Resolve user identities to a unique individual; and
c. Collect, validate, and verify identity evidence.

NOTE: Identity proofing is the process of collecting, validating, and verifying user's identity information for the purposes of issuing credentials for accessing a system.

IA-12(2) - Identity Proofing | Identity Evidence (M, O)
For systems categorized as Moderate, or higher

Require evidence of individual identification be presented to the registration authority.

NOTE: Acceptable forms of evidence are consistent with the risk to the systems, roles, and privileges associated with the user's account.

IA-12(3) - Identity Proofing | Identity Evidence Validation and Verification (M, O)
For systems categorized as Moderate, or higher

Require that the presented identity evidence be validated and verified to a level consistent with the risk to the systems, roles, and privileges associated with the users account.

NOTE: Validation refers to the process of confirming that the evidence is genuine and authentic and that the data contained in the evidence is correct, current, and related to an actual person or individual.

IA-12(5) - Identity Proofing | Address Confirmation (M, O)
For systems categorized as Moderate, or higher

For users whose identity cannot be readily confirmed (i.e. users external to the agency), require that an out-of-band mechanism be used to confirm the user's address of record.

NOTE: Confirmation artifacts can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts is typically obtained from records, and not self-asserted by the user. The address can be physical or a digital. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.

INCIDENT RESPONSE – IR

IR-2 - Incident Response Training (L, *O*)

For all systems

a. Provide incident response training to system users, including contractors and consolidated data center personnel as applicable, which is consistent with assigned user roles and responsibilities. Training must include the ability to identify and report common indicators of an incident (CIS-17.9).
   1. Incident response training must be provided:
      i) Within 30 days of assuming an incident response role or responsibility;
      ii) When required by system changes; and
      iii) Annually thereafter; and
   2. Information regarding reporting system anomalies and incidents to the incident handling team must be included in routine employee awareness activities and training (CIS-19.6).

IR-3 - Incident Response Testing (M, *O*)

For systems categorized as Moderate, or higher

a. Exercise the incident response capability for systems at least annually to determine the incident response effectiveness.
   1. At a minimum, tabletop exercises must be performed;
   2. Exercises must test communication channels, decision making, and incident responder technical capabilities (CIS-19.7); and
   3. Document the results of the testing in an after-action report for the purposes of improving existing processes, procedures, and policies.

IR-3(2) - Incident Response Testing | Coordination With Related Plans (M, O)

For systems categorized as Moderate, or higher

Coordinate incident response testing with organizational elements responsible for related plans. Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Occupant Emergency Plans, and Critical Infrastructure Plans.

IR-4 - Incident Handling (L, *O*)

For all systems

a. Implement security incident handling capability that includes preparation, detection, 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, testing, and exercises; and
d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

NOTE: Organizations recognize that incident response capability is dependent on the capabilities of organizational systems and the mission/business processes supported by those systems, in conjunction with other statewide organizations. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and systems.

IR-4(1) - Incident Handling | Automated Incident Handling Processes (M, O)

For systems categorized as Moderate, or higher

Employ automated mechanisms to support the incident handling processes.

NOTE: Automated mechanisms supporting incident handling processes include, for example, online incident management systems; and tools that support collection of live response data, full network packet capture, and forensic analysis.

IR-4(10) - Incident Handling | Supply Chain Coordination (NS, O)
For systems categorized as Moderate, or higher

Coordinate incident-handling activities involving supply chain events with other organizations involved in the supply chain.

NOTE: Organizations involved in supply chain activities include, for example, system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities.

IR-5 - Incident Monitoring (L*, O*)

For all systems

Track and document system security incidents.

IR-6 - Incident Reporting (L*, O*)

For all systems

a. Require personnel to report suspected or actual security incidents to internal Agency incident response resources as soon as possible, but in no case later than one hour following discovery (CIS-19.4); and
b. Assemble and maintain third-party contact information (e.g. Law Enforcement, relevant government departments, vendors, ISAC partners), to be used to report a security incident (CIS-19.5).

IR-6(1) - Incident Reporting | Automated Reporting (M, O)
For systems categorized as Moderate, or higher

Employ automated mechanisms to assist in reporting security incidents. Examples of automated mechanisms include: Email notification, workflow process software, etc.

IR-6(2) - Incident Reporting | Vulnerabilities Related to Incidents (M, O)
For systems categorized as Moderate, or higher

Report vulnerabilities associated with security incidents to Agency System Owners, to ensure timely corrective action is taken.

IR-6(3) - Supply Chain Coordination (M, O)
For systems categorized as Moderate, or higher

Provide security incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.

IR-7 - Incident Response Assistance (L*, O*)

For all systems

Ensure access to appropriate organizational and statewide incident response resources for the purpose of handling and reporting of information security incidents. These resources may include access to forensic services, web-based support, and incident response capability.

IR-7(1) - Incident Response Assistance | Automation Support for Availability of Information and Support (M, O)
For systems categorized as Moderate, or higher

Employ automated mechanisms to increase availability of incident response information and support.

NOTE: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increased response capabilities and support.

IR-7(2) - Incident Response Assistance | Coordination With External Providers (NS, O)

For systems categorized as Moderate, or higher

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

IR-8 - Incident Response Plan (L, O)

For all systems

a. Develop Incident Response Plans (CIS-19.1), that:
   1. Provide agencies with a roadmap for implementing an incident response capability, and how that capability coordinates with the Enterprise Security Office;
   2. Describe the structure and organization of the incident response capability, including management personnel, incident response roles, and key decision-makers (CIS-19.3);
   3. Explicitly designate responsibility for incident response to specific individuals or positions (CIS-19.2);
   4. Provide a high-level description of how the incident response capability fits into the overall organization and coordinates with the Oregon Enterprise Security Office and the Statewide Incident Response Plan;
   5. Meet the unique requirements of the Agency, which relate to mission, size, structure, functions, and regulated data;
   6. Define reportable incidents and create an incident scoring and prioritization schema based on known or potential impact to prioritize remediation and define escalation procedures and frequency of status updates (CIS-19.8);
   7. Provide metrics for measuring the incident response capability within each agency;
   8. Ensure tracking and documentation of incident response efforts from initiation through resolution (CIS-19.2);
   9. Define the resources and management support needed to effectively maintain and mature an incident response capability; and
   10. Are reviewed and approved by senior leadership, information security representatives, regulatory and compliance representatives, and applicable Incident Response Team leaders and personnel.
b. Distribute copies of the Incident Response Plan(s) to organizational senior leadership, operational and information security personnel, regulatory and compliance personnel, and personnel possessing significant incident response responsibilities;
c. Review the Incident Response Plan(s) annually;
d. Update and revise the Incident Response Plan(s) to address system and organizational changes, and problems encountered during plan implementation, testing, or execution; and
e. Communicate changes to the Incident Response Plan(s) to agency senior leadership, operational security personnel, regulatory and compliance personnel, and personnel possessing significant incident response responsibilities.

IR-9 - Information Spillage Response (M, *O*)

For systems categorized as Moderate, or higher

a. Respond to information spills by:
   1. Identifying the specific information involved in the system contamination;
   2. Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill;

3. Isolating the contaminated system or system component;
4. Eradicating the information from the contaminated system or component; and
5. Identifying other systems, or system components, including disaster recovery and back-up systems and information, that may have been subsequently contaminated.

NOTE: Information spillage refers to instances where protected information is inadvertently placed on systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to a system and then is subsequently determined to be of higher sensitivity.

MAINTENANCE (MA)

MA-2 - Controlled Maintenance (L, *O*)

For all systems

a. Schedule and perform maintenance and repairs on system components in accordance with manufacturer or vendor specifications and Agency requirements.
   1. The maintenance schedule and procedures must be documented;
   2. Scheduled maintenance must include controls to monitor the completion of maintenance in accordance with the system's documented maintenance schedule and vendor recommendations; and
   3. If a manufacturer, vendor, or developer provided maintenance schedule does not exist, the system must be reviewed at least every three months in order to determine if maintenance is required.

b. Approve and monitor all maintenance activities under all circumstances:
   1. Whether performed on-site or remotely; and
   2. Whether the equipment is serviced on-site or removed to another location.

c. Receive explicit approval from the Agency System Owner for the removal of any system or system component from organizational facilities for off-site maintenance or repairs. ETS is the "Agency" for system components under their control;

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

e. Following maintenance, repair, or replacement actions:
   1. Check all potentially impacted security and privacy controls to verify that the controls are still functioning properly; and
   2. Check all potentially impacted systems and applications to verify that they are still functioning properly; and

f. Document maintenance and repair activities, including non-local maintenance and diagnostics, and review the records quarterly.

MA-3 - Maintenance Tools (M, *O*)

Enterprise wide

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

NOTE: Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware and software packet sniffers.

MA-3(1) - Maintenance Tools | Inspect Tools (M, O)

Enterprise wide

Inspect all maintenance tools carried into the facility by maintenance personnel for improper modifications.

MA-3(2) - Maintenance Tools | Inspect Media (M, O)

For systems categorized as Moderate, or higher

Check all media containing diagnostic and test programs for malicious code before use in the system.

MA-3(3) - Maintenance Tools | Prevent Unauthorized Removal (M, O)

For systems categorized as Moderate, or higher

a. Prevent the unauthorized removal of system maintenance equipment containing data classified at level 3 (Restricted) or greater in one of the following ways:
   1. Verify that there is no Agency information contained on the equipment;

2. Sanitizing the equipment;
3. Retaining the equipment securely within the facility; or
4. Obtaining an exemption from the Agency System Owner explicitly authorizing the removal of the equipment from the facility.

MA-4 - Nonlocal Maintenance (L, *O*)

For all systems

a. Approve and monitor all non-local maintenance and diagnostic activities performed on Agency systems;
b. Allow the use of non-local maintenance and diagnostic tools, only as consistent with statewide and agency policy, and that are documented in the system security plan;
c. Employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
d. Maintain records of non-local maintenance and diagnostic activities; and
e. Upon completion of non-local maintenance and diagnostic activities, the following must be completed and verified:
   1. Terminate all sessions and network connections invoked in the performance of the activity;
   2. Disable or close all temporarily enabled or opened maintenance ports, services, or protocols; and
   3. Disable all temporary access.

MA-5 - Maintenance Personnel (L, *O*)

For all systems

Agencies must:

a. Maintain a list of authorized maintenance organizations and personnel. The list must be updated immediately upon notification of personnel changes (refer to Personnel Security controls), and reviewed at least quarterly;
b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorization; and
c. Designate personnel with required access authorization and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorization.

MA-6 - Timely Maintenance (M, *O*)

For systems categorized as Moderate, or higher

Obtain maintenance support and / or spare parts in sufficient time to meet recovery time objectives.

MEDIA PROTECTION (MP)

MP-2 - Media Access (L*, O*)

For all systems

Restrict access to all digital and non-digital media to authorized personnel only.

MP-3 - Media Marking (L*, O*)

Enterprise wide

a. Label removable system media to indicate the distribution limitations and handling caveats according to the type of information that the media contains.
   1. Mark removable system media containing information of mixed classification levels with the classification level corresponding to the highest level of information stored on the media. For example, if the media contains data ranging from classification Level 1 through Level 3, the media must be labeled as Level 3 and handled accordingly;
   2. Protect unmarked media according to the highest asset classification standard until the type of information stored on the media has been determined, and the media marked; and
   3. System personnel and users must mark documents with appropriate classification labels so that it is immediately apparent that the information must be protected from unauthorized disclosure.

MP-4 - Media Storage (M*, O*)

For systems categorized as Moderate, or higher

a. Physically control and securely store all digital and non-digital media within defined controlled areas using defined security measures; and
b. Protect all system media until the media's destruction or sanitization via approved equipment, techniques, and procedures.

NOTE: System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external or removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm.

MP-5 - Media Transport (M*, O*)

Enterprise wide for information classified at Level 3 (Restricted) or above:

a. Protect digital and non-digital media at all times during transport outside of controlled areas using defined security measures (locked container, approved encryption technologies, etc.);
b. Maintain accountability for system media during transport outside of controlled areas. Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering;
c. Document activities associated with the transport of system media. Organizations establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records; and
d. Restrict the activities associated with the transport of system media to authorized personnel.

MP-6 - Media Sanitization (L*, O*)

Enterprise-wide

a. Sanitize all system media (both digital and non-digital) using OSCIO approved equipment, techniques, and procedures prior to disposal, release out of organizational control, or reuse.
   1. Media containing information classified at Level 3 (Restricted) and above must not be reused;

2. Media and information that is subject to ongoing e-discovery, litigation, or other legal requirements must not be sanitized, disposed of, or destroyed; and
3. Non-digital media containing Level 3 (Restricted) information must be destroyed upon completion of use, by shredding using an OSCIO approved shredder, or media destruction contractor. Non-digital media containing Level 4 (Critical) information must be destroyed immediately upon completion of use, on-site by authorized personnel; and

b. Ensure that the strength and integrity of the sanitization methods employed is commensurate with the security category or data classification of the information contained on the media.

MP-6(1) - Media Sanitization | Review / Approve / Track / Document / Verify (H, O)

For systems categorized as Moderate, or higher

Review, approve, track, document, and verify disposal actions for media containing Level 3 (Restricted) or Level 4 (Critical) information.

MP-7 - Media Use (L*, O*)

For all systems

a. Prohibit the use of non-approved media on state systems. Only OSCIO approved media types are allowed to be used on state systems.
   1. If no documented and approved business need exists to support the use of external removable media, systems must be configured not to write information to such devices (CIS-13.8); and
   2. If removable storage devices are required based on an approved and documented business need, enterprise software must be used that can configure systems to allow the use of specific devices. An inventory of such devices must be maintained (CIS-13.7); and

b. Prohibit the use of portable storage devices on organizational systems, when such devices have no identifiable owner.

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

PE-2 - Physical Access Authorizations (L*, O*)

Enterprise wide

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where systems and data reside;
b. Issue authorization credentials (e.g. badges, RFID keycards, mechanical keys) for facility access;
c. Review the access list detailing authorized facility access by individuals at a minimum annually; and
d. Remove individuals from the facility access list when access is no longer required.

PE-3 - Physical Access Control (L*, O*)

Enterprise wide

a. Enforce physical access authorizations for all physical access points (including designated entry and exit points) to areas where systems reside.
   1. Individual access authorizations must be verified before access to areas where information classified at Level 2 and above is stored or accessed;
   2. Facility access must be controlled using physical access control devices (e.g. keys, locks, combinations, RFID card readers, etc.)
      i) All facilities must have at least one physical security control protecting it from unauthorized access, damage, or interference;
      ii) Facilities that process or store information classified at Level 3 (Restricted) or higher must employ multiple layers of physical security controls; and
      iii) For areas used to process or store information classified at Level 3 (Restricted) or higher, maintain access logs for controlled entry points;

   NOTE: Agencies have flexibility in the types of access logs employed. Access logs can be manual, automated, or some combination thereof.
b. Authorized personnel must authenticate visitors before authorizing visitor access to physically secure locations, must escort visitors, and monitor visitor activity at all times;
c. Secure all keys, combinations, and other physical access control devices, and perform an inventory at least annually;
d. Change combinations at least annually, or when combinations are compromised, individuals are transferred or terminated; and
e. Re-key locks when physical keys are lost or compromised.

PE-4 - Access Control for Transmission (M*, O*)

For systems categorized as Moderate, or higher

a. Control physical access to system distribution and transmission lines; and
b. Include protective measures to control physical access to information system distribution and transmission lines, such as:
   1. Locked wiring closets;
   2. Disconnected or locked spare jacks; and
   3. Protection of cabling by conduit or cable trays.

NOTE: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or modification of unencrypted transmissions while in transit.

PE-5 - Access Control for Output Devices (M*, O*)

For systems categorized as Moderate, or higher

Control physical access to information from output devices (e.g. monitors, printers, audio devices) to prevent unauthorized individuals from obtaining the information.

NOTE: Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only; placing output devices in locations that can be monitored by organizational personnel; installing monitor or screen filters; and using headphones. Output devices include, for example, monitors, printers, copiers, scanners, facsimile machines, and audio devices.

PE-6 - Monitoring Physical Access (L*, O*)

Enterprise wide

a. Monitor physical environment access to the facility where the system resides to detect and respond to physical security incidents;
b. Review physical environment access logs at least monthly and upon occurrence of indications of inappropriate or unusual activity indicating an elevated need for audit review; and
c. Coordinate results of reviews and investigations with the organizational incident response capability.

PE-6(1) - Intrusion Alarms / Surveillance Equipment (M, O)

For areas with systems or data (digital or non-digital) classified at Level 3 (restricted), or higher

Monitor physical access to the area where the data resides using physical intrusion alarms and surveillance equipment.

PE-8 - Visitor Access Records (L*, O*)

For all systems

a. Maintain visitor access records for the facility where the system resides.
   1. Visitor access logs must contain the following data elements:
      i) Name of the visitor;
      ii) Organization of the visitor;
      iii) Form of identification used by the visitor;
      iv) Date of access;
      v) Time of entry;
      vi) Time of departure;
      vii) Purpose of visit;
      viii) Name of the person visited; and
      ix) Organization of the person visited; and
   2. Access logs must be retained for at least five years; and
b. Review visitor access records at least monthly.

PE-9 - Power Equipment and Cabling (M*, O*)

For systems categorized as Moderate, or higher

Protect power equipment and power cabling for the system from damage and destruction.

PE-10 - Emergency Shutoff (M*, O*)

For systems categorized as Moderate, or higher

a. Provide the capability of shutting off power to the system or individual system components in emergency situations;
b. Place emergency shutoff switches or devices in locations as defined by applicable standards, to facilitate safe and easy access for personnel; and
c. Protect emergency power shutoff capability from unauthorized activation.

NOTE: This control applies primarily to facilities containing concentrations of system resources including, for example, data centers, server rooms, rooms/buildings containing computer-controlled machinery, and mainframe computer rooms.

PE-11 - Emergency Power (M*, O*)

For systems categorized as Moderate, or higher

Provide a short-term 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 (L*, O*)

For all systems

Employ and maintain automatic emergency lighting 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 (L*, O*)

For all systems

Employ and maintain fire suppression and detection devices/systems that are supported by an independent energy source.

NOTE: Fire suppression and detection devices or systems that may require an independent energy source include, for example, sprinkler systems, fixed fire hoses, and smoke detectors.

PE-13(1) - Detection Devices and Systems (M, O)

For areas with systems or data (digital or non-digital) classified at Level 3 (restricted), or higher

Employ fire detection devices/systems for the system that activate automatically and notify designated agency personnel and emergency responders in the event of a fire.

PE-13(2) - Automatic Suppression Devices and Systems (M, O)

For areas with systems or data (digital or non-digital) classified at Level 3 (restricted), or higher

a. Employ fire suppression devices/systems for the system that provide automatic notification of any activation to designated agency personnel and emergency responders; and
b. Employ an automatic fire suppression capability for the system when the facility is not staffed on a continuous basis.

PE-14 - Temperature & Humidity Controls (L*, O*)

For all systems

a. Maintain the temperature and humidity levels within the facility where the system resides within limits as documented by the equipment manufacturer; and
b. Continuously monitor, in real-time, temperature and humidity levels within the facility where the system resides.

NOTE: This control applies primarily to facilities containing concentrations of system resources including, for example, data centers, server rooms, rooms/buildings containing computer-controlled machinery, and mainframe computer rooms.

PE-15 - Water Damage Protection (L*, O*)

For all systems

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.

NOTE: This control applies primarily to facilities containing concentrations of system resources including, for example, data centers, server rooms, rooms/buildings containing computer-controlled machinery, and mainframe computer rooms.—Use the 'footnote version'

PE-16 - Delivery and Removal (L*, O*)

For all systems

a. Authorize, monitor, and control information system components entering and exiting the facility and maintain records of those items:
   1. Delivery and loading areas and other points where unauthorized persons could access state agency buildings are restricted to identified and authorized personnel; and
   2. Monitored, reviewed and audit supplier service delivery.

PE-17 - Alternate Work Site (M*, O*)

For systems categorized as Moderate, or higher

a. Determine and document the alternate worksites allowed for use;
b. Employ statewide and agency security controls at alternate work sites;
c. Assess the effectiveness of security controls at alternate work sites; and
d. Provide a means to communicate with information security personnel in case of security incidents or problems.

PE-18 - Location of System Components (H*, O*)

For systems categorized as Moderate, or higher

Position system components within facilities to minimize potential damage from physical and environmental hazards, and to minimize opportunities for unauthorized access.

PLANNING (PL)

PL-2 - Security Plans (L, *O*)

For all systems

a. Develop system security plans that:
   1. Are consistent with the organization's enterprise architecture;
   2. Explicitly define the authorization boundary for the system;
   3. Describe the operational context of the system in terms of missions and business processes;
   4. Provide the security categorization of the system including supporting rationale;
   5. Describe the operational environment for the system and relationships with or connections to other systems;
   6. Provide an overview of the security requirements for the system;
   7. Identify any relevant overlays (e.g. manufacturer, name, IP address, etc.), for appropriate distribution, if applicable;
   8. Describe the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
   9. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distribute copies of the system security plan(s) and communicate subsequent changes to the plans to designated Agency personnel;

c. Review the system security plan(s) on an annual basis;

d. Update the security plan(s) to address changes to the system and environment of operation or problems identified during plan implementation or security control assessments; and

e. Protect the security plan(s) from unauthorized disclosure and modification.

PL-2(3) - Plan / Coordinate With Other Organizational Entities (M, O)

For systems categorized as Moderate, or higher

Plan and coordinate security-related activities affecting the system with appropriate agency information security oversight, change management, and other stakeholders, before conducting such activities to reduce the impact on other organizational entities that may be affected by changes to the system.

PL-4 - Rules of Behavior (L, *O*)

For all systems

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 every three years; and

d. Require individuals to read and re-sign when the rules of behavior are revised or updated, or at least annually.

PL-4(1) - Rules of Behavior | Social Media and Networking Restrictions (L, O)

For all systems

Include explicit restrictions on the use of social media and networking sites, and the posting of organizational information on public websites.

NOTE: This control addresses the rules of behavior related to the use of social media and networking sites when organizational personnel are using such sites for official duties or in the conduct of official business; when organizational information is involved in social media and networking transactions; and when personnel are accessing social media and networking sites from organizational systems.

PL-8 - Security Architecture (L*, O*)

For all systems

a. Develop security architecture for the system that:
   1. Describe the philosophy, requirements, and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
   2. Describe how the security architecture is integrated into and supports the enterprise architecture; and
   3. Describe any security-related assumptions about, and dependencies on, external services;

b. Review and update the security architecture for the system every three years to reflect updates in the enterprise architecture, or any time there is a significant change to the system; and

c. Reflect planned security architecture changes in the system security plan.

PL-10 - Baseline Selection (L*, O*)

For all systems

Select a control baseline (Low, Moderate, or Moderate +) for the system.

PL-11 - Baseline Tailoring (L*, O*)

For all systems

Tailor the selected control baseline by applying specified tailoring actions. After selecting an appropriate control baseline, organizations initiate a tailoring process to align the controls more closely with the specific protection needs and concerns of their stakeholders, or local, state, and federal regulatory requirements.

PROGRAM MANAGEMENT (PM)

PM-1 - Information Security Program Plan (O)

Enterprise wide

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 the organization-wide information security program plan annually;

c. Update the information security program plan to address organizational changes and problems identified during plan implementation or control assessments; and

d. Protect the information security program plan from unauthorized disclosure and modification.

PM-4 - Plan of Action and Milestones Process (O)

For all systems

a. Implement a process to ensure that plans of action and milestones (see CA-5) for the agency security programs and associated organizational systems:
   1. Are developed and maintained;
   2. Document the remedial information security and privacy action to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the State; and
   3. Are reported in accordance with established reporting requirements; and

b. Review plans of action and milestones for consistency with organizational risk management strategy and organization-wide priorities for risk response actions.

NOTE: The plan of action and milestones is a key document in the information security and privacy programs and is subject to reporting requirements established by the Office of Management and Budget. Organizations view plans of action and milestones from an enterprise-wide perspective, **prioritizing risk response actions** and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities.

PM-5 - System Inventory (L*, O)*

For all systems

Develop, document, and maintain an inventory of all organizational systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of agency information to allow the agency to regularly review its information assets and ensure, to the extent reasonably practicable, that such information is accurate, relevant, timely, and complete.

a. Develop and maintain an inventory of all hardware assets whether connected to the Agency's network or not (CIS-1.4).
   1. Utilize an active discovery tool to identify devices connected to the Agency's network, and update the Agency's hardware asset inventory as appropriate (CIS-1.1);
   2. Utilize a passive discovery tool to identify devices connected to the Agency's network, and update the Agency's hardware asset inventory as appropriate (CIS-1.2);
   3. Where Dynamic Host Configuration Protocol (DHCP) is used, employ logging on all DHCP servers or IP address management tools to support updating the organization's hardware asset inventory (CIS-1.3);

4. Ensure that the asset inventory includes information determined to be necessary by the Agency to achieve effective property accountability, including but not limited to:
   i) Network address;
   ii) Hardware (MAC) address;
   iii) Machine name;
   iv) Asset owner (including agency, division, department, program, etc.);
   v) Date and time that the asset record was last updated in the inventory; and
   vi) Network connectivity that is authorized for the asset (CIS-1.5);
5. Ensure that unauthorized components are removed from the network, quarantined, or the inventory is updated to reflect that the component is unauthorized, in a timely manner (CIS-1.6);
6. Review and update the list of authorized components:
   i) Utilizing automated tools or manual processes;
   ii) At a minimum annually;
   iii) When required due to system upgrades or other significant changes; and
   iv) As an integral part of system component installations;
7. Maintain an up to date inventory of all Agency network boundaries (i.e. points of ingress and egress) (CIS-12.1):
   i) This inventory must include a list of all authorized wireless access points connected to the Agency's network (CIS-15.1); and
8. The inventory must include a list of each of the organization's authentication systems, including those located onsite or at a remote service provider (CIS-16.1); and

b. Develop and maintain an inventory of all software that is required in the enterprise for any business purpose on any business system (CIS-2.1):
   1. Ensure that only software applications or operating systems currently supported by the software's vendor are added to the Agency's authorized software inventory. Software currently in use and no longer supported must be identified as unsupported in the inventory system (CIS-2.2);
   2. Utilize software inventory tools throughout the organization to support the documentation of all software on Agency systems (CIS-2.3);
   3. Ensure that the following items are tracked in the software inventory system:
      i) Name;
      ii) Version;
      iii) Publisher;
      iv) Agency System Owner(s);
      v) Term / End of Support; and
      vi) Install date for all software, including operating systems authorized by the organization (CIS-2.4);
   4. Tie the software inventory system to the hardware asset inventory so all devices and associated software are tracked (CIS-2.5);
   5. Ensure that the inventory includes a list of each of the organization's authentication systems, including those located onsite or at a remote service provider (CIS-16.1);
   6. Ensure that unauthorized software is removed, or the inventory is updated to reflect that the software is unauthorized, in a timely manner (CIS-2.6); and
   7. Review and update the list of authorized software programs:
      i) At a minimum annually;
      ii) When required due to system upgrades or other significant changes; and
      iii) As an integral part of system component installations.

NOTE: This control refers to an organization-wide inventory of systems, not system components as described in CM-8.

PERSONNEL SECURITY (PS)

PS-2 - Position Risk Designation (L, *O*)

Enterprise wide

a. Assign a risk designation to all organizational positions:
   1. The following must be considered regarding position risk designations:
      i) Program-level risk must be factored into the position risk designation;
      ii) The risk level associated with each user role that has access to the system must be assessed; and
      iii) A position's risk designation must consider:
         (1) Physical access to the system's hardware or software;
         (2) Physical or logical access to Level 3 (Restricted) or higher data;
         (3) The ability to override or bypass security controls;
         (4) The scope of IT resources potentially impacted by security violations; and
         (5) The FIPS 199 security categorization of the system;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations annually, or when a change to or addition of duties occurs.

PS-3 - Personnel Screening (L, O)

Enterprise wide

a. Perform screening on individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, standards, guidance, and the criteria established relative to any regulated data that the position requires access to.

PS-4 - Personnel Termination (L, O)

Enterprise wide

Upon termination of an individual's employment, agencies must:

a. Disable system access;
   1. If termination of employment is voluntary, terminate system access within the same day that employment is terminated; and
   2. If termination is involuntary, whenever possible, terminate system access just before or at the same time notification of such termination is provided to the employee, but in no case longer than two (2) hours following such notification;

b. Terminate / revoke any authenticators / credentials associated with the individual;

c. Upon departure counsel the terminated individual on continued obligations under system non-disclosure, confidentiality, or user access agreements;

d. Retrieve all security-related and agency system-related property (e.g. hardware authentication tokens, system administration and technical manuals, keys, identification / RFID cards, etc.);

e. Retain access to agency information and systems formerly controlled by the terminated individual; and

f. Notify appropriate agency personnel, including system management and facilities access, upon termination of the employee.

PS-5 - Personnel Transfer (L, *O*)

Enterprise wide

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 agency;

b. Initiate transfer or reassignment actions as appropriate following the formal transfer action for all personnel, including contractors;

c. Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify designated agency personnel, as required.

PS-6 - Access Agreements (L*, O*)

Enterprise wide

a. Develop and document access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements) for agency 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 at least annually.

PS-7 - Third-Party Personnel Security (L*, O*)

Enterprise wide

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

PS-8 - Personnel Sanctions (L*, O*)

Enterprise wide

a. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures:
   1. The sanctions process must be consistent with applicable federal and state laws, Executive Orders, directives, agreements, policies, regulations, standards, and guidance where applicable; and
b. Notify designated agency personnel when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

RISK ASSESSMENT (RA)

RA-2 - Security Categorization (L, *O*)

For all systems

a. Categorize the system and information it processes, stores, and transmits;
   1. System classification must take into account:
      i) The classification of the information received, stored, or processed:
         (1) *Level 1 Published:* Low-sensitive information. Information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of agency employees, clients, and partners. The disclosure, alteration, or destruction of Level 1 information generally has a *low* impact on security;
         (2) *Level 2 Limited:* Sensitive information that may not be protected from public disclosure, but if made easily and readily available may jeopardize the privacy or security of agency employees, clients, or partners. The disclosure, alteration, or destruction of Level 2 information generally has a *Low* impact on security;
         (3) *Level 3 Restricted:* Sensitive information intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners, or individuals who otherwise qualify for an exemption. Information in this category may be accesses and used by internal parties only when specifically authorized to do so in the performance of their duties. The disclosure, alteration, or destruction of Level 3 information generally has a *moderate* impact on security; and
         (4) *Level 4 Critical:* Information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the named individual(s), agency employees, clients, partners, or cause major Harm to the agency. The disclosure, alteration, or destruction of Level 4 information generally has a *high* impact on security; and
      ii) The FIPS 199 categorization of the system;

b. Document the security categorization results including supporting rationale, in the system security plan; and

c. Verify that the authorizing official or designee reviews and approves the security categorization decision.

RA-3 - Risk Assessment (L, *O*)

Enterprise wide

a. Conduct a risk assessment, including the likelihood and magnitude of harm, from:
   1. The unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
   2. Problems arising from the processing of regulated data;

b. Document risk assessment results in a risk assessment report;

c. Disseminate risk assessment results to designated personnel as defined in the System Security Plan; and

d. Update the risk assessment at a minimum every three years, or when there are significant changes to a system, its environment of operation, or other conditions that may impact security.

RA-3(1) - Risk Assessment | Supply Chain Risk Assessment (M, O)

For systems categorized as Moderate, or higher

a. Assess supply chain risks associated with systems, system components, and system services; and

b. Update the supply chain risk assessment at a minimum every three years, or when there are significant changes to the relevant supply chain, when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

NOTE: Systems, system components, and system services also include hosted and cloud-based solutions.

RA-5 - Vulnerability Scanning (L, *O*)

For all systems

a. Scan for vulnerabilities using a current SCAP-compliant scanning tool on the system and hosted applications at least weekly, and when new vulnerabilities potentially affecting the system/applications are identified and reported (CIS-3.1);
b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting checklists and test procedures; and
   3. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from any additional security control assessments;
d. Remediate legitimate vulnerabilities in accordance with an organizational assessment:
   1. Utilizing a risk-rating process to prioritize the remediation of discovered vulnerabilities; and (CIS-3.7); and
   2. Comparing the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner (CIS-3.6);
e. Share information obtained from the vulnerability scanning process and security control assessments with designated agency officials to help eliminate similar vulnerabilities in other systems (i.e., systemic weaknesses or deficiencies); and
f. Employ vulnerability scanning tools that include the capability to regularly update the vulnerabilities to be scanned.

RA-5(2) - Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified (L, O)

For all systems

Update the system vulnerabilities to be scanned prior to a new scan, or when new vulnerabilities are identified and reported.

RA-5(5) - Vulnerability Scanning | Privileged Access (M, O)

For systems categorized as Moderate, or higher

a. Perform authenticated vulnerability scanning with agents running locally on each system, or with remote scanners that are configured with elevated rights on the system being tested, with the exception of systems where this is not feasible and such exceptions are approved by Agency System Owner or designee, and documented (CIS-3.2);
b. Use a dedicated account for authenticated vulnerability scans. Such accounts must not be used for any other administrative activities (CIS-3.3); and
c. Where feasible, tie the account used for authenticated vulnerability scans to specific machines, at specific IP addresses (CIS-3.3).

RA-7 - Risk Response (L, *O*)

For all systems

Respond to findings from security assessments, monitoring, and audits.

RA-9 - Criticality Analysis (M, *O*)

For systems categorized as Moderate, or higher

Identify critical system components and functions by performing a criticality analysis for, system components, or system services and document the analysis in the System Security Plan.

NOTE: Criticality Analysis is an end-to-end functional decomposition performed by systems engineers to identify mission critical functions and components. Includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system missions(s).

System and Services Acquisition (SA)

SA-2 - Allocation of Resources (L*, O*)

For all systems

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

NOTE: A system security plan is sufficient to meet the requirements of both "a." and "b."

SA-3 - System Development Life Cycle (L*, O*)

For all systems

a. Utilize a System Development Life Cycle (SDLC) methodology that includes information security considerations;
b. Define and document information security roles and responsibilities throughout the system development life cycle;
c. Identify positions having information security roles and responsibilities associated with the system; and
d. Integrate information security risk management processes into the SDLC.

SA-4 - Acquisition Process (L*, O*)

For all systems

a. Include the following requirements, explicitly or by reference, in acquisition contracts for systems, system components, or system services:
   1. Security functional requirements;
   2. Security strength of mechanism requirements (i.e. password length and complexity requirements, encryption strength, hardware security, etc.);
   3. Security assurance requirements;
   4. Security-related documentation requirements;
   5. Requirements for protecting security documents;
   6. Description of the system development environment and the environment in which the system is intended to operate;
   7. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and
   8. Security acceptance criteria.

SA-4(1) - Acquisition Process | Functional Properties of Security Controls (M, O)

For systems categorized as Moderate, or higher

Require the developer of the system, system component, or system service to provide a description of the functional properties of the security controls to be implemented.

NOTE: Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

SA-4(2) - Acquisition Process | Design and Implementation Information for Security Controls (M, O)

For systems categorized as Moderate, or higher

Require vendors and contractors to provide information in acquisition documents that describe the design and implementation details of the security controls to be employed within the system, system components, or system services (including functional interfaces among control components), with sufficient detail to permit independent analysis and testing of the controls.

SA-4(9) - Functions / Ports / Protocols / Services in Use (M, O)
For systems categorized as Moderate, or higher

Require developers of systems, system components, or system services to identify early in the SDLC, the functions, ports, protocols, and services that are intended for organizational use.

SA-5 - System Documentation (L, O)

For all systems

a. Obtain administrator documentation (whether published by a vendor/manufacturer or written in-house) 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 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 enable individuals to use the system, component, or service in a secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service of individuals;
c. When system documentation is either unavailable or non-existent, the following actions must be taken:
   1. Document attempts to obtain such documentation; and
   2. Recreate selected system documentation if such documentation is essential to the effective implementation and / or operation of security controls;
d. Protect documentation as required, in accordance with the organizational risk management strategy; and
e. Distribute documentation to appropriate agency personnel.

SA-8 - Security Engineering Principles (L*, O*)

For all systems

a. Apply system security engineering principles in the specification, design, development, implementation, and modification of the system.
b. Security engineering principles must include, but are not limited to:
   1. Establishing and testing secure coding practices appropriate to the programming language and development environment being used (CIS-18.1);
   2. Ensuring that explicit error checking is performed and documented for all input, including size, data type, and acceptable ranges or formats (CIS-18.2);
   3. Applying static and dynamic analysis tools to verify that secure coding practices are being adhered to (CIS 18.7);
   4. Developing layered protections;
   5. Establishing sound security methodology, architecture, and controls as the foundation for design;
   6. Incorporating security into all phases the System Development Life Cycle (SDLC);
   7. Delineating physical and logical security boundaries;
   8. Ensuring system developers and integrators are trained in secure software development;
   9. Tailoring security controls to meet organizational and operational needs;
   10. Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns, as well as compensating controls and design patterns needed to mitigate risk; and
   11. Enabling informed risk management decisions in order to reduce risk to acceptable levels; and
c. For legacy systems, apply the above security engineering principles to system upgrades and modifications, to the extent feasible given the current state of the hardware, software, and firmware components within the system.

SA-9 - External System Services (L*, O*)

For all systems

a. Require that providers of external system services comply with organizational security requirements and employ applicable agency-defined security controls;
b. Define and document agency oversight, user roles and responsibilities, and service levels, with regard to external system services; and
c. Employ agency defined processes, methods, and techniques to monitor security compliance by external service providers on an ongoing basis.

NOTE: This includes services that are used by, but not a part of, agency systems. Agencies establish relationships with external service providers in a variety of ways including, for example, through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges.

SA-9(2) - External System Services | Identification of Functions, Ports, Protocols, and Services (M, O)
For systems categorized as Moderate, or higher

Require providers of external system services to identify the functions, ports, protocols, and other services required for use.

SA-10 - Developer Configuration Management (M*, O*)

For systems categorized as Moderate, or higher

a. Require the developer of the system, system component, or system service to:
   1. Perform configuration management throughout the system development lifecycle, including: design; development; system test; and unit acceptance test;
   2. Document, manage, and control the integrity of changes throughout the system development lifecycle, including: design; development; system test; and unit acceptance test;
   3. Implement only organization-approved changes to the system, component, or service;
   4. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
   5. Track security flaws and flaw resolution within the system, component, or service and report findings to appropriate personnel as identified in the system security plan.

SA-11 - Developer Security Testing and Evaluation (M*, O*)

For systems categorized as Moderate, or higher

a. Require the developer of the system, system component, or system service, at all post-design phases of the system development life cycle, to:
   1. Create and implement a security assessment plan, and document the security assessment plan in the system security plan;
   2. Perform security testing and evaluation according to the security assessment plan;
   3. Implement a verifiable flaw remediation process that includes accepting and addressing reports of software vulnerabilities discovered during assessments (CIS-18.8); and
   4. Correct flaws identified during testing and evaluation.

SA-12 - Supply Chain Risk Management (M*, O*)

For systems categorized as Moderate, or higher

a. Employ safeguards 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; and
b. Select and document the implemented supply chain safeguards in the system security plan.

NOTE: Supply chain-related events include, for example: disruption, theft, insertion of counterfeits, insertion of malicious code, malicious development practices, improper delivery practices, and use of defective components.

SA-15 - Development Process, Standards, and Tools (M*, O*)

For systems categorized as Moderate, or higher

a. Require the developer of the system, system component, or system service to follow a documented development process that:
   1. Explicitly addresses security requirements;
   2. Identifies the standards and tools used throughout the development life cycle;
   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 least annually to determine if the process, standards, tools, tool options and tool configurations selected and employed comply with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

SA-22 - Unsupported System Components (L*, O*)

For all systems

a. Replace systems and system components when support for the system or component is no longer available from the manufacturer:
   1. Software acquired from external sources must be current and supported by the developer, or appropriately hardened based on the developer's security recommendations (CIS-2.2) (CIS-18.3); and
   2. Only current and trusted third-party system components may be used for software developed internally (CIS-18.4); and

b. Provide justification and documented approval for the continued use of unsupported systems or system components that are required to satisfy mission/business needs:
   1. To reduce the risk of running unsupported systems or system components to an acceptable level, compensating controls must be implemented and documented.

SYSTEM AND COMMUNICATION PROTECTION (SC)

SC-2 - Application Partitioning (M*, S*)

For systems categorized as Moderate, or higher

a. Separate user functionality, including user interface services, from system management functionality. System management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. Separation is accomplished by using one of the following methods, or a combination of methods, as applicable:
   1. Different computers;
   2. Different central processing units;
   3. Different instances of operating systems;
   4. Different network addresses; and
   5. Other methods, as appropriate.

SC-3 - Security Function Isolation (H*, S*)

For systems categorized as Moderate, or higher

Isolate system security functionality from non-security functionality in order to control access to and protect the integrity of the hardware, software, and firmware that performs security functionality. Systems must restrict access to security functions using access control mechanisms and by implementing least privilege capabilities.

SC-4 - Information In Shared System Resources (M*, S*)

For systems categorized as Moderate, or higher

Prevent unauthorized and unintended information transfer via shared system resources.

NOTE: This control refers to protecting data in any computing resource which may be accessed by multiple users or processes. The purpose of this control is to prevent information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. This control also applies to encrypted representations of information.

SC-5 - Denial of Service Protection (L*, S*)

For all systems

a. Configure systems, firewalls, routers, and other network infrastructure to protect against or limit the effects of Denial of Service (DoS) attacks; and
b. Guard against, limit, reduce the susceptibility to, and detect DoS attacks utilizing methods such as:
   1. Configuring systems according to documented and established standards for minimizing the effects of DoS attacks;
   2. Configuring routers and switches to disable forwarding of packets to broadcast addresses, as applicable; and
   3. Configuring routers and firewalls to filter traffic.

SC-7 - Boundary Protection (L*, S*)

For all systems

a. Monitor and control communications:
   1. At the external boundary of the system;
   2. At key internal boundaries within the system:
      i) Firewalls must be placed in front of any critical servers in order to verify and validate traffic going to the server. Any unauthorized traffic must be blocked and logged (CIS-9.5);

ii) Monitoring systems at each of the organization's network boundaries must be configured to record network packets passing through the boundary (CIS-12.5); and

iii) Intrusion Detection Systems (IDS) sensors must be deployed to look for unusual attack mechanisms and detect compromise of systems at each of the organization's network boundaries (CIS-12.6).

b. Deploy publicly accessible system components (e.g., public web servers) in separate networks or sub-networks with separate network interfaces;

c. Implement a separate wireless network for personal or untrusted devices. Enterprise network access from this network must be prohibited and audited accordingly (CIS-15.10); and

d. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices (e.g. proxies, gateways, routers, firewalls, encrypted tunnels);

SC-7(3) - Boundary Protection | Access Points (M, S)
For systems categorized as Moderate, or higher

Limit the number of external network connections to the system.

SC-7(4) - Boundary Protection | External Telecommunications Services (M, O)
For systems categorized as Moderate, or higher

a. Implement a managed interface for each external telecommunication service;
b. Establish a traffic flow policy for each managed interface;
c. Employ security controls as needed to 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/business need and duration of that need; and
e. Review exceptions to the traffic flow policy at least annually and remove exceptions that are no longer supported by an explicit mission/business need.

SC-7(5) - Boundary Protection | Deny by Default / Allow by Exception (M, S)
For systems categorized as Moderate, or higher

Deny network traffic by default and allow network traffic by documented policy (i.e. deny all, permit by exception). Access must be limited to trusted and necessary IP address ranges and ports / protocols at each of the organization's network boundaries (CIS-12.3) (CIS-12.4).

SC-7(7) - Boundary Protection | Prevent Split Tunneling For Remote Devices (M, S)
For systems categorized as Moderate, or higher

Prevent split tunneling.

NOTE: For the purpose of this control, split tunneling is defined as the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an **uncontrolled external network**. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks.

SC-7(8) - Boundary Protection | Route Traffic to Authenticated Proxy Servers (M, S)
For systems categorized as Moderate, or higher

a. Route all network traffic to or from the Internet through an authenticated application layer proxy that is configured to filter unauthorized connections (CIS-12.9); and
b. Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the traffic content. A whitelist may be used to document authorized sites that are allowed to be accessed through the proxy without decrypting the traffic (CIS-12.10).

SC-7(10) - Boundary Protection | Prevent Exfiltration (NS, S)
For systems categorized as Moderate, or higher

a. Prevent the exfiltration of information:
   1. Automated tools must be deployed at network perimeters to monitor for unauthorized transfer of sensitive information and block such transfers while alerting information security personnel (CIS-13.3); and
   2. Monitor all traffic leaving the organization and detect any unauthorized use of encryption (CIS-13.5); and

b. Conduct and document the results of exfiltration tests at least annually.

SC-7(11) - Boundary Protection | Restrict Incoming Communications Traffic (NS, S)
For systems categorized as Moderate, or higher

a. Allow incoming communications only from agency authorized / allowed sources to be routed to agency authorized / allowed destinations. Authorized / allowed sources and destinations must include, at a minimum, consideration of IP addresses, ports, and protocols; and
b. Deploy Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the agency's external network boundaries (CIS-12.7).

SC-7(12) - Boundary Protection | Host-Based Protection (NS, S)
For all systems

Implement host-based boundary protection mechanisms on end systems (e.g. servers, workstations, laptops, and mobile devices) using a default-deny rule that drops all traffic except those services and ports that are explicitly allowed (CIS-9.4).

SC-7(14) - Boundary Protection | Protect Against Unauthorized Physical Connections (NS, S)
For all systems

Protect against unauthorized physical connections.

NOTE: For example, where systems operating at different security categories share common space within a facility, or common physical and environmental controls (e.g. common equipment rooms, wiring closets, and cable distribution paths).

Mechanisms to protect against unauthorized physical connections include, but are not limited to: Physical access controls enforcing limited authorized access to systems operating at the higher classification level (e.g. server cages, port locks, usb locks), clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces.

SC-7(21) - Boundary Protection | Isolation of System Components (H, O/S)
For systems categorized as Moderate, or higher

a. Employ boundary protection mechanisms to physically or logically segregate systems according to the assessed level of risk to the organization (CIS-2.10);
b. Require system administrators to use a dedicated machine for all administrative tasks or tasks requiring administrative access. The machine must be segmented from the organization's primary network and not allowed Internet access. The machine must not be used for routine business functions, including but not limited to: reading e-mail, composing documents, etc. (CIS-4.6);
c. Require network engineers to use a dedicated machine for all administrative tasks or tasks requiring administrative access. The machine must be segmented from the organization's primary network and not allowed Internet access. The machine must not be used for routine business functions, including but not limited to: reading e-mail, composing documents, etc. (CIS-11.6);
d. Require management of the infrastructure, including network devices, industrial control devices, and physical security systems, to occur across network connections that are separated from the business use of that network, relying on separate VLANs or, if possible, on entirely different physical connectivity for management sessions(CIS-11.7); and
e. Maintain separate environments for production and non-production environments (CIS-18.9).

SC-8 - Transmission Confidentiality and Integrity (M*, S*)

For systems categorized as Moderate, or higher

Protect the confidentiality and integrity of transmitted information.

SC-8(1) - Transmission Confidentiality and Integrity | Cryptographic or Alternate physical Protection (M, S)

For systems categorized as Moderate, or higher

Implement FIPS 140-2 (level 1 or greater as required according to regulatory standards) cryptographic mechanisms to prevent unauthorized disclosure of information, and to detect changes to information during transmission across the WAN and within the Agency LAN (CIS-14.4).

NOTE: Some regulated data requirements may require the use of a FIPS 140-2 *certified* (as opposed to compliant) mechanism.

SC-10 - Network Disconnect (M*, S*)

For systems categorized as Moderate, or higher

Terminate the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity. This control applies to network connections associated with specific communications sessions for both internal and external networks.

SC-12 - Cryptographic Key Establishment and Management (L, O/S)

For all systems

a. Establish and manage cryptographic keys for required cryptography employed within the system in accordance with Agency defined requirements for key generation, distribution, storage, access, and destruction. This may be performed using manual procedures or automated mechanisms with supporting manual procedures:
    1. Key management requirements must be defined in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, specifying appropriate options, levels, and parameters; and
    2. Trust stores must be managed to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems; and
    3. Public key certificates must be issued by using a secure process that both verifies the identity of the certificate holder, and ensures that the certificate is issued to the intended party.
b. Revoke a certificate within 24 hours if the associated private key is compromised, and as soon as possible when the certificate is no longer needed.

SC-13 - Cryptographic Protection (L*, S*)

For all systems

a. Implement required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance (CIS-18.5):
    1. Data classified at Level 3 or greater must employ a FIPS 140-2 validated encryption algorithm for data in transit and at rest;
    2. Agencies shall document the FIPS certificate number for the encryption employed; and
    3. The NIST validation website shall be checked at least annually, or when planning upgrades, to ensure that product validations have not been revoked, and that usage is still valid; and
b. Encrypt information at rest using a tool that requires a secondary authentication mechanism not integrated into the operation system, in order to access the information (CIS-14.8).

NOTE: Information classified as Level 3 (Restricted) or greater must be encrypted in transit and at rest, including on mobile devices (CIS-13.9).

SC-15 - Collaborative Computing Devices (L, S)

For all systems

a. Prohibit remote activation of collaborative computing devices (e.g. networked white boards, cameras, microphones); and
b. Provide an explicit indication to the users physically present at the devices that the collaborative computing devices are in use.

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

SC-17 - Public Key Infrastructure (M*, O/S*)

For systems categorized as Moderate, or higher

a. Obtain public key certificates from an OSCIO approved service provider; or
b. Issue public key certificates under an agency-documented PKI Certificate Policy (CP) and Certification Practice Statement (CPS).

SC-18 - Mobile Code (M, O)

For systems categorized as Moderate, or higher

a. Define acceptable and unacceptable mobile code and mobile code technologies;
b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorize, monitor, and control the use of mobile code within systems used to receive, transmit, store, or process regulated data, or any information classified as Level 3 (Restricted) or higher.

NOTE: Mobile code technologies include, for example, Java, JavaScript, ActiveX, Portable Document Format (PDF) files, Postscript, Shockwave movies, Flash animations, and VBScript. A related term is "active content," which may refer to program code embedded in a web page or to plug-in applications intended for use in the web browser.

SC-18(4) - Mobile Code | Prevent Automatic Execution (NS, S)

For all systems

Disable auto-execute features on system components that employ portable storage devices (e.g. Compact Disks (CD), Digital Video Disks (DVD), and Universal Serial Bus (USB) drives) (CIS-8.5).

SC-19 - Voice over Internet Protocol (M*, O*)

Enterprise wide

a. Establish usage restrictions and implementation guidelines for Voice over Internet Protocol (VoIP) technologies
    1. Utilize virtual local area networks (VLAN) technology to segment Voice over Internet Protocol (VoIP) traffic from all other traffic; and
    2. All communications on the VoIP network involving data classified at Level 3 (Restricted) or above must comply with all applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance, including encryption; and
b. Authorize, monitor, and control the use of VoIP technologies within the system.

SC-20 - Secure Name / Address Resolution Service (Authoritative Source) (L*, S*)

For all systems

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.

NOTE: This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

SC-21 - Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L*, S*)

For all systems

The follow control applies if the system is Internet-facing. 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 & Provisioning for Name / Address Resolution Service (L*, S*)

For all systems

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 (M*, S*)

For systems categorized as Moderate, or higher

Protect the authenticity of communications sessions.

NOTE: This control addresses communications protection at the session, versus packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks and session hijacking, and the insertion of false information into sessions.

SC-28 - Protection of Information at Rest (M*, S*)

For systems categorized as Moderate, or higher

Implement mechanisms to ensure the confidentiality and integrity of information at rest (CIS-13.9).

SC-28(1) - Protection of Information at Rest | Cryptographic Protection (M, S)

For systems categorized as Moderate, or higher

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information classified as Level 3 (Restricted) or above (CIS-13.9). Organizations have the flexibility to encrypt all information on storage devices or encrypt specific data structures including, for example, files, records, or fields.

SC-39 - Process Isolation (L*, S*)

For all systems

Maintain a separate execution domain for each executing process with the system.

NOTE: Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is readily available in most commercial operating systems that employ multi-state processor technologies.

SC-41 - Port and I/O Device Access (NS*, O*)

For systems categorized as Moderate, or higher

a. Create and maintain a list of authorized connection ports or input / output devices; and
b. Physically or logically disable or remove any unauthorized connection port or input /output device.

NOTE: Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVD) drives.

SYSTEM AND INFORMATION INTEGRITY (SI)

SI-2 - Flaw Remediation (L*, O*)

For all systems

a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects prior to installation;
c. Apply security-relevant software and firmware updates within a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw as follows: (CIS-11.4)
   1. Flaws rated as High and above severity within seven (7) calendar days;
   2. Medium severity within fifteen (15) calendar days; and
   3. All others within thirty (30) calendar days; and
d. Incorporate flaw remediation into organizational configuration management processes.

SI-2(2) - Flaw Remediation | Automated Flaw Remediation Status (M, O)

For systems categorized as Moderate, or higher

Employ automated mechanisms to determine the state of system components with regard to flaw remediation, including automated software update tools to ensure that operating systems and third-party software on all systems are running the most recent security updates provided by the software vendor (CIS-3.4) (CIS-3.5).

SI-3 - Malicious Code Protection (L*, O*)

For all systems

a. Employ malicious code protection mechanisms at system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network;
b. Automatically update malicious code protection mechanisms (including signature definitions) whenever new releases are available and in accordance with agency-wide configuration management policy, procedures, and standards (CIS-8.2); and
c. Configure malicious code protection mechanisms to:
   1. Perform periodic scans of the system at least weekly, and real-time scans of files as the files are downloaded, opened, or executed;
   2. Automatically scan removable media when inserted or connected (CIS-8.4); and
   3. Block malicious code at gateways and quarantine at host; validate quarantined code before releasing to user; and clean quarantined malware as appropriate.

SI-3(1) - Malicious Code Protection | Central Management (M, O)

For all systems

Centrally manage anti-malware software to continuously monitor and defend each of the Agency's workstations and servers (CIS-8.1).

SI-4 - System Monitoring (L*, O/S*)

For all systems

a. Monitor events to detect:
   1. Attacks and indicators of potential attack; and
   2. Unauthorized local, network, and remote connections;
b. Identify unauthorized use of the system (CIS-4.9);
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. Protect information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion;
e. Adjust the level of system monitoring activity accordingly whenever there is an indication of increased risk to state operations, assets, individuals, organizations, or the nation, based on law enforcement information, intelligence information, or other credible sources of information;
f. Provide system monitoring information to personnel or roles designated by the agency as needed to support the agency's continuous monitoring and incident response programs;

SI-4(2) - System Monitoring | Automated Tools for Real-Time Analysis (M, S)

For systems categorized as Moderate or higher

Employ automated tools and mechanisms to support near real-time analysis of events.

NOTE: Automated tools and mechanisms include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or Security Information and Event Management technologies that provide real time analysis of alerts and notifications generated by organizational systems.

SI-4(4) - System Monitoring | Inbound and Outbound Communications Traffic (M, S)

For systems categorized as Moderate or higher

Monitor outbound communications traffic at the external boundary of the information system and selected interior points within the network (e.g., subnetworks, subsystems) for unusual or unauthorized activities.

NOTE: Unusual or unauthorized activities within agency information systems include: large file transfers; long-time persistent connections; use of unusual protocols and ports; and attempted communications with suspected malicious external addresses.

SI-4(5) - System Monitoring | System Generated Alerts (M, S)

For systems categorized as Moderate or higher

a. Alert appropriate personnel or roles, as defined in system security plans, when indicators of compromise occur. This includes but is not limited to:
   1. Presence of malicious code;
   2. Unauthorized export of information;
   3. Signaling to an external information system;
   4. Indicators of potential intrusion;
   5. Any incident relevant to the Oregon CITPA;
   6. Successful phishing attack;
   7. Denial of service attack;
   8. Adding an account to or removing an account from any group with administrative privileges; and (CIS-4.8)
   9. Unsuccessful login attempts to an account with administrative privileges (CIS-4.9).

NOTE: Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated or they may be transmitted, for example, telephonically, by electronic mail messages, or by text messaging.

SI-4(11) - System Monitoring | Analyze Communications Traffic Anomalies (NS, O/S)

For systems categorized as Moderate, or higher

Analyze outbound communications traffic at the external boundary of the system to detect anomalies. Anomalies within agency systems include, for example, large file transfers, long-time persistent connections, unauthorized use of encryption, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

SI-4(14) - System Monitoring | Wireless Intrusion Detection (H, S)
For systems categorized as Moderate, or higher

Employ wireless intrusion detection systems (WIDS) to detect attack attempts and potential compromises or breaches of the system, and alert on unauthorized wireless access points connected to the organization's network (CIS-15.3).

SI-4(23) - System Monitoring | Host-Based Devices (M, O)
For systems categorized as Moderate, or higher

Implement host-based monitoring mechanisms (e.g., Host intrusion detection system (HIDS), file integrity monitoring mechanisms, behavioral analytics, etc.) on information systems that receive, process, store, or transmit information classified at Level 3 (Restricted) or higher.

SI-5 - Security Alerts, Advisories, and Directives (L, *O*)

For all systems

a. Receive system security alerts, advisories, and directives from OSCIO/ESO on an ongoing basis. Sources may include, but are not limited to: US-CERT, ICS-CERT, and MS-ISAC;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate security alerts, advisories, and directives to appropriate Agency personnel, including Agency System Owners; and
d. Implement security directives in accordance with established timeframes. OSCIO must be notified of the degree of non-compliance.

SI-7 - Software, Firmware, and Information Integrity *(M, O/S)*

For systems categorized as Moderate, or higher

a. Employ integrity verification tools, including Security Content Automation Protocol (SCAP) compliant configuration monitoring systems, to detect unauthorized changes to software and information (CIS-5.5):
   1. Verify all security configuration elements;
   2. Catalog approved exceptions; and
   3. Detect and alert when unauthorized changes occur.

SI-7(1) - Software, Firmware, and Information Integrity | Integrity Checks (M, S)
For systems categorized as Moderate, or higher

Perform an integrity check of software, firmware, and information as defined in applicable agency system security plans.

SI-7(7) - Software, Firmware, and Information Integrity | Integration of Detection and Response (M, O)
For systems categorized as Moderate, or higher

Incorporate the detection of unauthorized changes into the organizational incident response capability. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of system privileges.

SI-8 - Spam Protection (M, *O*)

For systems categorized as Moderate or higher

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

SI-8(1) - Spam Protection | Central Management (M, O)
For systems categorized as Moderate or higher

Centrally manage spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the agency-defined, centrally managed spam protection controls.

SI-8(2) - Spam Protection | Automatic Updates (M, S)
For systems categorized as Moderate or higher

Automatically update spam protection mechanisms.

SI-10 - Information Input Validation (M*, S*)

For systems categorized as Moderate or higher

Check the validity of defined information inputs. System inputs include, for example, character set, length, numerical range, acceptable values, and verification that inputs match specified definitions for format and content.

NOTE: Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

SI-11 - Error Handling (M*, S*)

For systems categorized as Moderate or higher

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 authorized personnel or roles as defined in the applicable system security plan.

SI-12 - Information Management & Retention (L*, O*)

For all systems

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.

SI-16 - Memory Protection (M*, S*)

For systems categorized as Moderate, or higher

Implement security safeguards to protect the system memory from unauthorized code execution. For example, anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) available in operating systems, or appropriate toolkits deployed that can be configured to apply protection to a broader set of applications and executables (CIS-8.3).