Information Technology (IT) Configuration Management (CM) Standard

February 9, 2024

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **IAS_Governance@ed.gov**.

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2024.02.10 16:06:17 -05'00'

Steven Hernandez
Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Date	Summary of Changes
1.0	1/14/2022	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/31/2022	Update to incorporate feedback from IAS; address security measures required by Executive Order (EO) 14028, and OMB regulations and memoranda and updated NIST guidance issued in response to EO 14028.
1.2	2/11/2022	Update overlay for CM-9 and CM-10.
1.3	2/10/2023	Annual review. Cleanup of formatting throughout. Updated hyperlink for OMB A-130 and added footnote and link for DHS HVA Controls. Updated CM-3(4) to remove requirement for low baseline. Updated CM-5(1) to align with NIST 800-53 Rev5. Clarified overlay requirements for CM-2(7) ED-01, CM-7(2) ED-01, CM-8(1), and CM-9. Added Control Overlay CM-8 ED-04 to address M-22-09 requirements. Changed CM-2(7) ED-02 to reserved and removed overlay requirements.
5.4	2/9/2024	Aligned document major version number to align with NIST SP 800-53 revision number. Clean up formatting and numbering throughout and update broken links. Section 2, Standards was updated to include the description of incorporating organizationally defined parameters (ODP) for controls that may be necessary from external control overlays (e.g., High Value Assets [HVA]). Inserted references to NIST SP 800-53B tailoring guidance. Updated Section 4, Acronyms as appropriate. Updated language in controls CM-01, CM-02(07), CM-03, CM-03(04), CM-03(06), CM-04 ED-03, CM-05, CM-05(01), CM-06, CM-07, CM-08, CM-08 ED-01, CM-08 ED-04, CM-11, and CM-12. Added controls CM-03(07), CM-05(05), CM-07(09), CM-13, and CM-14. Rescinded control CM-02(07) ED-04. Added “leading zeros” to control identifiers in alignment with patch release of NIST SP 800-53 (Release 5.1.1) to applicable controls, enhancements, and overlays.

Table of Contents

1 INTRODUCTION

This governance document establishes U.S. Department of Education (ED or Department) information technology (IT) system configuration management standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders (EO), Emergency Orders, Binding Operational Directives (BOD), and Department Administrative Communications System Directives (ACSD) and Handbooks. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing governance Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standards (FIPS) Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as amended, as baseline information system controls.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these system configuration management standards control standards.

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2 STANDARDS

The Department standards for IT system configuration management controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS PUB 199 categorization level (e.g., Low [L], Moderate [M] and High [H]) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS PUB 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS PUB 199 impact-level or privacy baseline.

In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax information (FTI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075[5], *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information.* Systems that are Federal Risk and Authorization Management Program (FedRAMP) authorized must implement and comply with the FedRAMP identified baselines[6].

Throughout the standard, there are controls captured that have not been scoped to any specific security or privacy baseline. This is intentional as all controls for identified external overlays and baselines (e.g., FedRAMP, IRS, HVA), that may apply to systems within the Department, have been incorporated into the standard. This ensures the organization defined parameters (ODPs) for controls within the Department have been clearly defined in a consistent manner.

Based upon an assessment of risk and determination that the level of protection for the security-relevant information within a system is not adversely impacted, controls identified in the current version of NIST SP 800-53B that support only the integrity security objective may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if not defined in a lower baseline).

This standard directly supports the Department's integration of the NIST Cybersecurity Framework (CSF) and NIST Privacy Framework (PF) by using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to *APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY* for a summary of controls by baseline and corresponding NIST CSF and NIST PF categories and subcategories.

[5] IRS Publication 1075 https://www.irs.gov/pub/irs-pdf/p1075.pdf
[6] FedRAMP baselines https://www.fedramp.gov/baselines/

2.1 CM-01 Policy and Procedures (P, L, M, H)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in ACSD-OCIO-004[7], *Cybersecurity Policy* a Department-level IT Configuration Management policy (e.g., this document) that:

a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

b. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

c. authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as ACSD-OCIO-004, Cybersecurity Policy.

The Department CISO in conjunction with the Senior Agency Official for Privacy (SAOP) are designated to manage the development, documentation, and dissemination of the Department-level IT Configuration Management policy.

This policy shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office Information System Owners (ISO) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of the Department's IT Configuration Management policy and the associated controls. The ISO and ISSO shall review IT Configuration Management procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

[7] Also known as OCIO: 3-112

2.2 CM-02 Baseline Configuration (L, M, H)

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

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

   1. At a minimum annually (i.e., each fiscal year);

   2. When required due to significant system change; and

   3. When system components are installed or upgraded.

2.2.1 CM-02(02) Baseline Configuration | Automation Support for Accuracy and Currency (M, H)

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using applicable manual and automated tools designated by the PO and approved for use by the Enterprise Architecture Technical Insertion, (EA(TI)).

2.2.2 CM-02(03) Baseline Configuration | Retention of Previous Configurations (M, H)

Retain at a minimum one (1) previous version of baseline configuration of the system to support rollback.

2.2.3 CM-02(07) Baseline Configuration | Configure Systems and Components for High-risk Areas (M, H, and Control Overlay)

a. Issue a hardened device with a temporary network and email alias for the duration of travel, at the discretion of the ED Security Operations Center (EDSOC), to individuals traveling to locations that the organization deems to be of significant risk; and

b. Perform the following actions on Government Furnished Equipment and Services (GFES) which traveled outside of the United States and its territories upon the user's return from travel:

   1. Examination for signs of tampering;

   2. Reimaging of the hard drive;

   3. Scanning for malware; and

c. Other actions deemed necessary by the EDSOC based upon the foreign travel location(s).

Control Overlay CM-02(07) ED-01 (M, H): Permit ED Government Furnished Equipment and Services (GFES) to be taken (equipment) or used (services) outside of the United States and its territories only after explicit authorization via the Foreign Travel Request (FTR), or Domestic Employee Teleworking Overseas (DETO) IT request form.

Control Overlay CM-02(07) ED-02: Reserved

Control Overlay CM-02(07) ED-03 (M, H): Disapprove requests to take or use standard issued GFES in any country on the Department's sensitive country list (SCL). Users traveling to a country on the Department's SCL are required to use a separate hardened device with a temporary network and email alias for the duration of travel.

Control Overlay CM-02(07) ED-04 (M, H): Scan all devices prior to travel and conduct or coordinate activities required by the EDSOC to ensure the assigned GFES is authorized for foreign travel, properly configured, and secured before travel begins.

Control Overlay CM-02(07) ED-05 (M, H): Ensure GFES laptops have an approved Department Virtual Private Network (VPN) installed prior to travel. Require users to test connection and operability of their devices and the VPN solution before travel.

2.3 CM-03 Configuration Change Control (M, H, and Control Overlay)

a. Determine and document the types of changes to the system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

c. Document configuration change decisions associated with the system;

d. Implement approved configuration-controlled changes to the system;

e. Retain records of configuration-controlled changes to the system for a minimum of 6 months;

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through the ED Configuration Change Board (CCB) or CCB approved alternate that convenes at a minimum monthly or in accordance with ED CCB process documentation.

Control Overlay CM-03 ED-01 (L, M, H): Use configuration management practices to maintain EO-critical software platforms and all software deployed to those platforms; control and monitor the platforms and software to ensure the configuration is not changed outside of change control processes.

2.3.1 CM-03(01) Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes (H)

Use ED approved automated mechanisms to:

a. Document proposed changes to ED systems;

b. Notify the ED Configuration Change Board (CCB) or CCB approved alternate, ISO, and ISSO of proposed changes to the system and request change approval;

c. Highlight proposed changes to the system that have not been approved or disapproved within time period specified in the change management process documentation;

d. Prohibit changes to the system until designated approvals are received;

e. Document all changes to the system; and

f. Notify the ED CCB, ISO, and ISSO when approved changes to the system are completed.

2.3.2 CM-03(02) Configuration Change Control | Testing, Validation, and Documentation of Changes (M, H)

Test, validate, and document changes to the system before finalizing the implementation of the changes.

2.3.3 CM-03(04) Configuration Change Control | Security and Privacy Representatives (M, H)

Require ED required security and privacy representatives to be members of the CCB.

2.3.4 CM-03(06) Configuration Change Control | Cryptography Management (H)

Ensure that cryptographic mechanisms used to provide encryption, identification, authentication, and authorization are under configuration management.

2.3.5 CM-03(07) Configuration Change Control | Review System Changes

Review changes to the system at least twice a year or when dictated by the ED configuration change control process to determine whether unauthorized changes have occurred.

2.4 CM-04 Impact Analyses (P, L, M, H and Control Overlays)

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Control Overlay CM-04 ED-01 (L, M, H): Use current authorized version of the ED Security Impact Analysis (SIA) template prior to change implementation, to determine whether a proposed change to an existing system is minor or significant and what residual risk, if any, needs to be treated as part of the change.

Control Overlay CM-04 ED-02 (L, M, H): Conduct, analyze and evaluate for adverse impact on security in the case of emergency / unscheduled changes.

Control Overlay CM-04 ED-03 (L, M, H): Conduct independent risk assessments to determine impact to existing authorizations to operate for all SIAs which identify a major change is proposed or has been implemented under an emergency change; major changes are defined as one or more of the following:

a. System boundary changes which result in one or more of the following:

   1. New internal or external interconnection(s)

   2. New public-facing internet protocol (IP) address(es) or Uniform Resource Locator(s) (URLs)

3. Addition of one or more new subsystems
4. Transfer of system ownership which results in a new Authorizing Official.

b. Addition, modification, or deletion of one or more NIST SP 800-60 business area and associated information types that changes the system security categorization.

c. Change to common infrastructure, support services or environment of operation including the addition of or change to one or more of the following:

1. Service providers
2. Physical data centers
3. Cloud service providers (e.g., platform as a service [PaaS] or software as a service [SaaS] changing infrastructure as a service [IaaS] provider; changing from one IaaS to a different IaaS such as moving from Amazon Web Services [AWS] to Azure; or PaaS provider changes such as Salesforce to Adobe)
4. Use of new services (e.g., ticketing system, monitoring system, etc.) regardless of whether internal or external
5. Cloud service provider loss of Federal Risk and Authorization Management Program (FedRAMP) authorization

d. Addition of new hardware, firmware or software that does not have a corresponding Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG).

e. Addition or removal of controlled unclassified information (CUI), including personally identifiable information (PII).

f. Changes to system function or essential mission/business functions supported.

g. Changes to the system architecture including but not limited to:

1. Addition of a new network device, server, or appliance (virtual or physical), service, middleware application, etc. which increases capability as it does not currently exist in the authorized boundary and has not been approved for use through Enterprise Program Management Review (EPMR) and Change Advisory Board (CAB) processes.
2. Migration to a different operating system, database, web application (e.g., Windows to Linux, Structured Query Language [SQL] database to Oracle, Internet Information Services [IIS] to Apache, client/server to web services).
3. Removal of system components without implementation of replacement components.
4. Merger with another system.

2.4.1 CM-04(01) Impact Analyses | Separate Test Environments (H)

Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.

2.4.2 CM-04(02) Impact Analyses | Verification of Controls (M, H)

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

2.5 CM-05 Access Restrictions for Change (L, M, H)[8]

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

2.5.1 CM-05(01) Access Restrictions for Change | Automated Access Enforcement and Audit Records (H)[8]

a. Enforce access restrictions using ED approved automated mechanisms; and

b. Automatically generate audit records of the enforcement actions

2.5.2 CM-05(05) Access Restrictions for Change | Privilege Limitation for Production and Operation

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

2.6 CM-06 Configuration Settings (L, M, H, and Control Overlays

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using the most updated DISA STIG, with Security Engineering and Architecture Branch (SEA) authorized deviations as needed;

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for individual components within systems including, but not limited to, servers, workstations, network components and databases based on explicit operational requirements which are documented in the system security plan (SSP) and/or secure configuration baseline; and

[8] CM-05 and CM-05(01) have been identified by NIST SP 800-53B as supporting only integrity and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Control Overlay CM-06 ED-01 (L, M, H): Use the following configuration standards, in the order of precedence shown, when a DISA STIG is not available for a product or system:

a. NIST standards and baselines;

b. Other U.S. Government standards;

c. Cybersecurity industry best practices, benchmarks, and guidelines (i.e., Center for Internet Security, or CIS); and

d. Vendor checklists and baselines.

Control Overlay CM-06 ED-02 (L, M, H): Conduct independent verification and validation of all recommended deviations from the DISA STIG and, if warranted, request and receive authorization for use of these deviations from the Department CISO or authorized delegate.

Control Overlay CM-06 ED-03 (L, M, H): Identify and implement the proper hardened security configuration for each EO-critical software platform and all software deployed to that platform and use the configuration to enforce the principles of least privilege, separation of duties, and least functionality.

2.6.1 CM-06(01) Configuration Settings | Automated Management, Application, and Verification (H)

Manage, apply, and verify configuration settings for key components of infrastructure, to include but not limited to, network servers, desktops and databases related to those information systems based on mission requirements running within the FISMA system boundary using ED approved automated mechanisms.

2.6.2 CM-06(02) Configuration Settings | Respond to Unauthorized Changes (H)

Take the following actions in response to unauthorized changes to approved baseline configuration settings:

a. Alert designated organizational personnel including the EDSOC, ISO, ISSO;

b. Restore established configuration settings; or

c. In extreme cases, halt affected information system processing.

2.7 CM-07 Least Functionality (L, M, H, and Control Overlays)

a. Configure the system to provide only mission essential capabilities; and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: those not needed to conduct business as specified in ED minimum security baselines (e.g., Hypertext Transfer Protocol [HTTP], teletype network [Telnet], File Transfer Protocol

[FTP]); DISA STIGs; NIST standards and baselines; other U.S. Government standards; cyber security industry best practices, benchmarks, and guidelines; and vendor checklists and baselines, as determined to be appropriate by the CISO

Control Overlay CM-07 ED-01 (L, M, H): Disable maintenance ports when not in use.

2.7.1 CM-07(01) Least Functionality | Periodic Review (M, H)

a. Review the system at a minimum annually for non-HVA systems, and quarterly for HVA systems, to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

b. Disable or remove identified functions, ports, protocols, software and services within the system deemed to be unnecessary and/or non-secure by the CISO.

2.7.2 CM-07(02) Least Functionality | Prevent Program Execution (M, H, and Control Overlay)

Prevent program execution in accordance with ED defined policies regarding software program usage and restrictions, to include but not limited to:

a. ED authorized software programs (i.e., allow-list); and

b. ED unauthorized software programs (i.e., deny-list) only in circumstances where it is technologically infeasible to deploy and operate the allow-list.

Control Overlay CM-07(02) ED-01 (L, M, H): Configure email protocols and services to implement least functionality principles.

2.7.3 CM-07(05) Least Functionality | Authorized Software (M, H)

a. Identify software programs authorized to execute on ED information systems;

b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

c. Review and update the list of authorized software programs at a minimum annually (i.e., each fiscal year

2.7.4 CM-07(09) Least Functionality | Prohibiting the Use of Unauthorized Hardware

a. Identify hardware components authorized for system use;

b. Prohibit the use or connection of unauthorized hardware components;

c. Review and update the list of authorized hardware components at least annually.

2.8 CM-08 System Component Inventory (L, M, H, and Control Overlay)

a. Develop and document an inventory of system components that:

   1. Accurately reflects the system;
   2. Includes all components within the system;
   3. Does not include duplicate accounting of components or components assigned to any other system;
   4. Is at the level of granularity deemed necessary for tracking and reporting; and
   5. Includes the following information to achieve system component accountability: as defined in Cyber Security Assessment and Management (CSAM) System Information, Appendix S – Hardware Listing and System Information, Appendix T – Software Listing; not required for cloud service providers or Shared Services.

b. Review and update the system component inventory at a minimum quarterly.

Control Overlay CM-08 ED-01 (L, M, H): Maintain a current inventory of systems, hardware, software assets, and information (data) under each Principal Office's (PO's) control throughout the respective system development lifecycles.

Control Overlay CM-08 ED-02 (L, M, H): Require all hardware and software to be approved by the EA(TI) for use on Department computers (laptop, desktop, server computers, and all other electronic devices) and networks.

Control Overlay CM-08 ED-03 (L, M, H): Identify, document, and quarterly update an inventory of critical software in accordance with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity, i*nclude in the inventory the system/platform where the EO-critical software resides and implement security measures for critical software required by NIST.

Control Overlay CM-08 ED-04 (L, M, H): Create ongoing, reliable and complete asset inventories and confirm asset presence on the network using the Continuous Diagnostics and Mitigation (CDM) program Hardware and Software Asset Management Tools (Layer A tools), per OMB M-22-09.

2.8.1 CM-08(01) System Component Inventory | Updates During Installation and Removal (M, H, and Control Overlays)

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

Control Overlay CM-08(01) ED-01 (L): Update the inventory of system components as part of component installations, removals, and system updates.

2.8.2 CM-08(02) System Component Inventory | Automated Maintenance (H)

Maintain the currency, completeness, accuracy, and availability of the inventory of system components using the Department's system of record for system inventory.

2.8.3 CM-08(03) System Component Inventory | Automated Unauthorized Component Detection (M, H)

a. Detect the presence of unauthorized hardware, software, and firmware components within the system using ED defined automated mechanisms; and

b. Take the following actions when unauthorized components are detected:

   1. Isolate the components; and

   2. Notify the Information System Security Officer (ISSO).

2.8.4 CM-08(04) System Component Inventory | Accountability Information (H)

Include in the system component inventory information, a means for identifying by name, Principal Office (PO), position, and role, individuals responsible and accountable for administering those components.

2.9 CM-09 Configuration Management Plan (M, H, and Control Overlay)

Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by Information System Owner (ISO) and Information System Security Officer (ISSO); and

e. Protects the configuration management plan from unauthorized disclosure and modification.

Control Overlay CM-09 ED-01 (M, H): Use the current version of the Department approved Configuration Management Plan (CMP) template to develop and maintain the plan required by this control; use of these templates is not required for cloud service providers and Shared Services.

2.10 CM-10 Software Usage Restrictions (L, M, H, and Control Overlay)

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

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

Control Overlay CM-10 ED-01 (L, M, H): Require users to seek approval or obtain a waiver for any unapproved software within 30 days.

Control Overlay CM-10 ED-02 (L, M, H): Replace components when support is no longer available from the developer, vendor, or manufacturer, unless extended support is obtained from either the component developer or third-party service supplier certified by the original component developer.

Control Overlay CM-10 ED-03 (L, M, H): Disapprove, remove, retire, or establish an acceptance of risk (AoR) for outdated ED system components.

Control Overlay CM-10 ED-04 (L, M, H): Provide documented justification and obtain approval (via a plan of action and milestones [POA&M] or AoR signed by the Authorizing Official [AO]) for the continued use of unsupported system components required to satisfy mission/business needs. Make all exception and waiver requests using the Risk Acceptance Form (RAF).

2.11 CM-11 User-Installed Software (L, M, H)

a. Establish policies as specified in ACSD-OCIO-011[9], *Software Asset Management Acquisition Policy* and ED Acceptable Use, as necessary, documenting permitted and prohibited actions regarding software installation and procedural enforcement methods governing the installation of software by users;

b. Enforce software installation policies through the following methods:

   1. Automated methods (e.g., configuration settings implemented on organizational systems); and

   2. Manual methods (e.g., periodic examination of user accounts);

c. Monitor policy compliance through the continuous monitoring process.

[9] Also known as OCIO: 3-110

2.12 CM-12 Information Location (M, H)

a. Identify and document the location of sensitive data as determined by the CISO or Chief Privacy Officer (CPO)/SAOP and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

2.12.1 CM-12(01) Information Location | Automated Tools to Support Information Location (M, H)

Use automated tools to identify sensitive information by information type on ED system components to ensure controls are in place to protect organizational information and individual privacy.

2.13 CM-13 Data Action Mapping

Develop and document a map of system data actions.

2.14 CM-14 Signed Components[10]

Prevent the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

[10] CM-14 has been identified by NIST SP 800-53B as supporting only integrity and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

4 ACRONYMS

Acronym	Definition
ACSD	Administrative Communications System Directives
AO	Authorizing Official
AoR	Acceptance of Risk
AWS	Amazon Web Services
BOD	Binding Operational Directive
CAB	Change Advisory Board
CCB	Configuration Change Board
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CIS	Center for Internet Security
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CM	Configuration Management Family
CMP	Configuration Management Plan
CPO	Chief Privacy Officer
CSAM	Cyber Security Assessment and Management
CSF	Cybersecurity Framework
CT.DM-P	Data Processing Management
CT.DP-P	Disassociated Processing
CT.PO-P	Data Processing Policies, Processes, and Procedures
CT-P	Control-P
CUI	Controlled Unclassified Information
DE	Detect
DE.AE	Anomalies and Events
DE.CM	Security Continuous Monitoring
DE.DP	Detection Processes
Department	U.S. Department of Education
DETO	Domestic Employee Teleworking Oversees
DHS	U.S. Department of Homeland Security
DISA	Defense Information Systems Agency
EA(TI)	Enterprise Architecture Technical Insertion
ED	U.S. Department of Education
EDSOC	ED Security Operations Center
EO	Executive Order
EPMR	Enterprise Program Management Review
FedRAMP	Federal Risk and Authorization Management Program
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FTI	Federal Tax Return Information
FTP	File Transfer Protocol
FTR	Foreign Travel Request
GFES	Government Furnished Equipment and Services

Acronym	Definition
GRP	Governance, Risk and Policy
GV.MT-P	Monitoring and Review
GV.PO-P	Governance Policies, Processes, and Procedures
GV-P	Govern-P
H	High
HTTP	Hypertext Transfer Protocol
HVA	High Value Asset
IaaS	Infrastructure As A Service
IAS	Information Assurance Services
ID	Identify
ID.AM	Asset Management
ID.IM-P	Inventory and Mapping
ID.RA-P	Risk Assessment
ID-P	Identify-P
IIS	Internet Information Services
IP	Internet Protocol
IRS	Internal Revenue Service
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
L	Low
M	Moderate
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
ODP	Organizationally Defined Parameters
OMB	Office of Management and Budget
P	Privacy
PaaS	Platform As A Service
PF	Privacy Framework
PII	Personally Identifiable Information
PO	Principal Office
POA&M	Plan of Action and Milestones
PR	Protect
PR.DS	Data Security
PR.DS-P	Data Security
PR.IP	Information Protection Processes and Procedures
PR.PO-P	Data Protection Policies, Processes, and Procedures
PR.PT	Protective Technology
PR.PT-P	Protective Technology
PR-P	Protect-P
PUB	Publication
RAF	Risk Acceptance Form
SaaS	Software As A Service
SAOP	Senior Agency Official for Privacy
SCL	Sensitive Country List
SEA	Security Engineering and Architecture Branch

Acronym	Definition
SIA	Security Impact Assessment
SP	Special Publication
SQL	Structured Query Language
SSP	System Security Plan
STIG	Security Technical Implementation Guide
Telnet	Teletype Network
URL	Uniform Resource Locator
VPN	Virtual Private Network

APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
CM-01	Policy and Procedures	X	X	X	X	PR.IP, DE.DP, GV.PO-P, GV.MT-P, PR.PO-P	PR.IP-1, DE.DP-2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P1
CM-02	Baseline Configuration		X	X	X	PR.DS, PR.IP, DE.AE, CT.DM-P, PR.PO-P, PR.DS-P	PR.DS-7, PR.IP-1, DE.AE-1, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.DS-P7
CM-02(02)	Baseline Configuration | Automation Support for Accuracy and Currency			X	X	PR.DS, PR.IP, DE.AE, CT.DM-P, PR.PO-P, PR.DS-P	PR.DS-7, PR.IP-1, DE.AE-1, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.DS-P7
CM-02(03)	Baseline Configuration | Retention of Previous Configurations			X	X	PR.DS, PR.IP, DE.AE, CT.DM-P, PR.PO-P, PR.DS-P	PR.DS-7, PR.IP-1, DE.AE-1, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.DS-P7
CM-02(06)	Baseline Configuration | Development and Test Environments					PR.DS, PR.IP, DE.AE, CT.DM-P, PR.PO-P, PR.DS-P	PR.DS-7, PR.IP-1, DE.AE-1, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.DS-P7

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
CM-02(07)	Baseline Configuration | Configure Systems and Components for High-risk Areas			X	X	PR.DS, PR.IP, DE.AE, CT.DM-P, PR.PO-P, PR.DS-P	PR.DS-7, PR.IP-1, DE.AE-1, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.DS-P7
CM-03	Configuration Change Control			X	X	PR.IP, DE.CM, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.PO-P2
CM-03(01)	Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes				X	PR.IP, DE.CM, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.PO-P2
CM-03(02)	Configuration Change Control | Testing, Validation, and Documentation of Changes			X	X	PR.IP, DE.CM, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.PO-P2
CM-03(03)	Configuration Change Control | Automated Change Implementation					PR.IP, DE.CM, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.PO-P2

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
CM-03(04)	Configuration Change Control | Security and Privacy Representatives			X	X	PR.IP, DE.CM, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.PO-P2
CM-03(05)	Configuration Change Control | Automated Security Response					PR.IP, DE.CM, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.PO-P2
CM-03(06)	Configuration Change Control | Cryptography Management				X	PR.IP, DE.CM, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.PO-P2
CM-03(07)	Configuration Change Control | Review System Changes					PR.IP, DE.CM, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.PO-P2
CM-03(08)	Configuration Change Control | Prevent or Restrict Configuration Changes					PR.IP, DE.CM, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.PO-P2

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
CM-04	Impact Analyses	X	X	X	X	PR.IP, GV.MT-P, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, GV.MT-P1, GV.MT-P5, CT.DM-P9, PR.PO-P1, PR.PO-P2
CM-04(01)	Impact Analyses | Separate Test Environments				X	PR.IP, GV.MT-P, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, GV.MT-P1, GV.MT-P5, CT.DM-P9, PR.PO-P1, PR.PO-P2
CM-04(02)	Impact Analyses | Verification of Controls			X	X	PR.IP, GV.MT-P, CT.DM-P, PR.PO-P	PR.IP-1, PR.IP-3, GV.MT-P1, GV.MT-P5, CT.DM-P9, PR.PO-P1, PR.PO-P2
CM-05	Access Restrictions for Change		X	X	X	PR.IP, PR.PO-P	PR.IP-1, PR.PO-P1
CM-05(01)	Access Restrictions for Change | Automated Access Enforcement and Audit Records				X	PR.IP, PR.PO-P	PR.IP-1, PR.PO-P1
CM-05(04)	Access Restrictions for Change | Dual Authorization					PR.IP, PR.PO-P	PR.IP-1, PR.PO-P1
CM-05(05)	Access Restrictions for Change | Privilege Limitation for Production and Operation					PR.IP, PR.PO-P	PR.IP-1, PR.PO-P1
CM-05(06)	Access Restrictions for Change | Limit Library Privileges					PR.IP, PR.PO-P	PR.IP-1, PR.PO-P1
CM-06	Configuration Settings		X	X	X	PR.IP, CT.DM-P, CT.DP-P, PR.PO-P	PR.IP-1, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DP-P4, PR.PO-P1
CM-06(01)	Configuration Settings | Automated Management, Application, and Verification				X	PR.IP, CT.DM-P, CT.DP-P, PR.PO-P	PR.IP-1, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DP-P4, PR.PO-P1

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
CM-06(02)	Configuration Settings | Respond to Unauthorized Changes				X	PR.IP, CT.DM-P, CT.DP-P, PR.PO-P	PR.IP-1, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DP-P4, PR.PO-P1
CM-07	Least Functionality		X	X	X	PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-1, PR.PT-3, PR.PO-P1, PR.PT-P2
CM-07(01)	Least Functionality | Periodic Review			X	X	PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-1, PR.PT-3, PR.PO-P1, PR.PT-P2
CM-07(02)	Least Functionality | Prevent Program Execution			X	X	PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-1, PR.PT-3, PR.PO-P1, PR.PT-P2
CM-07(03)	Least Functionality | Registration Compliance					PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-1, PR.PT-3, PR.PO-P1, PR.PT-P2
CM-07(04)	Least Functionality | Unauthorized Software					PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-1, PR.PT-3, PR.PO-P1, PR.PT-P2
CM-07(05)	Least Functionality | Authorized Software			X	X	PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-1, PR.PT-3, PR.PO-P1, PR.PT-P2
CM-07(06)	Least Functionality | Confined Environments with Limited Privileges					PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-1, PR.PT-3, PR.PO-P1, PR.PT-P2
CM-07(07)	Least Functionality | Code Execution in Protected Environments					PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-1, PR.PT-3, PR.PO-P1, PR.PT-P2
CM-07(08)	Least Functionality | Binary or Machine Executable Code					PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-1, PR.PT-3, PR.PO-P1, PR.PT-P2
CM-07(09)	Least Functionality | Prohibiting The Use of Unauthorized Hardware					PR.IP, PR.PT, PR.PO-P, PR.PT-P	PR.IP-1, PR.PT-3, PR.PO-P1, PR.PT-P2

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
CM-08	System Component Inventory		X	X	X	ID.AM, PR.DS, DE.CM, ID.IM-P, PR.DS-P	ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7, ID.IM-P1, ID.IM-P2, ID.IM-P7, PR.DS-P3
CM-08(01)	System Component Inventory | Updates During Installation and Removal			X	X	ID.AM, PR.DS, DE.CM, ID.IM-P, PR.DS-P	ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7, ID.IM-P1, ID.IM-P2, ID.IM-P7, PR.DS-P3
CM-08(02)	System Component Inventory | Automated Maintenance				X	ID.AM, PR.DS, DE.CM, ID.IM-P, PR.DS-P	ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7, ID.IM-P1, ID.IM-P2, ID.IM-P7, PR.DS-P3
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection			X	X	ID.AM, PR.DS, DE.CM, ID.IM-P, PR.DS-P	ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7, ID.IM-P1, ID.IM-P2, ID.IM-P7, PR.DS-P3
CM-08(04)	System Component Inventory | Accountability Information				X	ID.AM, PR.DS, DE.CM, ID.IM-P, PR.DS-P	ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7, ID.IM-P1, ID.IM-P2, ID.IM-P7, PR.DS-P3
CM-08(06)	System Component Inventory | Assessed Configurations and Approved Deviations					ID.AM, PR.DS, DE.CM, ID.IM-P, PR.DS-P	ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7, ID.IM-P1, ID.IM-P2, ID.IM-P7, PR.DS-P3

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
CM-08(07)	System Component Inventory | Centralized Repository					ID.AM, PR.DS, DE.CM, ID.IM-P, PR.DS-P	ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7, ID.IM-P1, ID.IM-P2, ID.IM-P7, PR.DS-P3
CM-08(08)	System Component Inventory | Automated Location Tracking					ID.AM, PR.DS, DE.CM, ID.IM-P, PR.DS-P	ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7, ID.IM-P1, ID.IM-P2, ID.IM-P7, PR.DS-P3
CM-08(09)	System Component Inventory | Assignment of Components to Systems					ID.AM, PR.DS, DE.CM, ID.IM-P, PR.DS-P	ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7, ID.IM-P1, ID.IM-P2, ID.IM-P7, PR.DS-P3
CM-09	Configuration Management Plan			X	X	PR.IP, CT.PO-P, PR.PO-P	PR.IP-1, CT.PO-P2, PR.PO-P1
CM-09(01)	Configuration Management Plan | Assignment of Responsibility					PR.IP, CT.PO-P, PR.PO-P	PR.IP-1, CT.PO-P2, PR.PO-P1
CM-10	Software Usage Restrictions		X	X	X	DE.CM	DE.CM-3
CM-10(01)	Software Usage Restrictions | Open-source Software					DE.CM	DE.CM-3
CM-11	User-installed Software		X	X	X	DE.CM	DE.CM-3
CM-11(02)	User-installed Software | Software Installation with Privileged Status					DE.CM	DE.CM-3
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring					DE.CM	DE.CM-3
CM-12	Information Location			X	X	ID.IM-P	ID.IM-P1, ID.IM-P7
CM-12(01)	Information Location | Automated Tools to Support Information Location			X	X	ID.IM-P	ID.IM-P1, ID.IM-P7

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
CM-13	Data Action Mapping					ID.IM-P, ID.RA-P, GV.MT-P	ID.IM-P1, ID.IM-P2, ID.IM-P3, ID.IM-P4, ID.IM-P5, ID.IM-P6, ID.IM-P7, ID.IM-P8, ID.RA-P1, ID.RA-P3, GV.MT-P1
CM-14	Signed Components						