IT Security Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05

Revision 6

March 3, 2025

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – July 13, 2005		
1	Heard/Scott	Changes made throughout the document to reflect FISMA, NIST and GSA Order CIO 2100.1B requirements.	Updated to reflect and implement various FISMA, NIST and GSA Order CIO 2100.1B requirements.	Various
2	Heard/Scott	Changes throughout the document to correspond with revisions made to CIO-IT Security-01-09, CIO-IT Security-01-03 and CIO-IT Security-01-04.	Updated to reflect the correlation of the CIO-IT Security Guides; and to further express policy within them as standalone documents.	Various
		Revision 2 – March 22, 2010		
1	Berlas/ Wood	Changes made throughout the document to reflect NIST and GSA requirements.	Updated to reflect and implement NIST SP 800-53 R3 and GSA requirements.	Various
		Revision 3 – July 14, 2015		
1	Riaz/Searcy	Changes made throughout the document to reflect NIST and GSA requirements.	Updated to reflect and implement the most current NIST SP 800-53 and GSA requirements.	Various
		Revision 4 – January 17, 2018		
1	Feliksa/ Klemens	Changes made throughout the document to reflect NIST and GSA requirements.	Updated to reflect GSA's current development and configuration management processes. Updated to align with Federal, NIST, and GSA guidance.	Throughout
		Revision 5 – March 1, 2022		
1	Dean/ Klemens	Revisions included: ● Updated to NIST SP 800-53, Revision 5 controls and GSA parameters. ● Updated format and content.	Align to current NIST guidance and GSA parameters. New or substantively changed controls from Revision 5 are: CM-1, CM-2, CM-2(2), CM-2(3), CM-3(1), CM-3(4), CM-3(6), CM-4(2), CM-5(1), CM-6, CM-6(1), CM-7, CM-7(1), CM-7(2), CM-8(2), CM-8(3), CM-9, CM-12, CM-12(1)	Throughout
		Revision 6 – March 3, 2025		
1	Klemens/ Peralta	Revisions included: ● Updated controls to add leading zeros and to align with the CTW. ● Moved CSF categories, Policy, References, and Roles and Responsibilities to Appendices. ● Added Security Impact Analysis template under CM-04. ● Updated guide to the latest guide format and style.	Aligned to current NIST and GSA guidance.	Throughout

Approval

IT Security Procedural Guide: Configuration Management (CM), CIO-IT Security-01-05, Revision 6, is hereby approved for distribution.

Signed by:
Dovarius Peoples
F107CD0700F2413...

Dovarius Peoples
Acting GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Table of Contents

Note: Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Appendix C.

1 Introduction

Systems operate in highly dynamic operating environments with frequent changes to hardware, software, firmware, or supporting networks. Configuration Management (CM) is a structured management and control process applied to the components of a system to manage the inevitable changes that occur during the system's life cycle. CM provides assurance that the system components are well defined and cannot be changed without proper justification and full knowledge of the consequences and allows the current configuration state of the system and its components to be accurately determined at any time.

CM assists in streamlining the change management process and prevents changes that could detrimentally affect the security posture of a system. In its entirety, the CM process reduces the risk that any changes made to a system compromise the system's confidentiality, integrity, or availability. Effective CM requires system changes be tested prior to implementation to observe the effects of the change, thereby minimizing the risk of adverse results. Without a disciplined process for controlling changes, Authorizing Officials (AOs) cannot be assured that systems under their purview will operate as intended, that defects will be minimized, and that system configuration management will be performed in a cost-effective or timely manner.

Every General Services Administration (GSA) system across all Service and Staff Offices (SSOs) must follow the CM practices identified in this guide. Any deviations from the security requirements established in GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," must be coordinated by the Information System Security Officer (ISSO) through the appropriate Information System Security Manager (ISSM) and authorized by the AO. Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form.

The CM principles and practices described in this guide are based on guidance from the National Institute of Standards and Technology (NIST) including NIST Special Publication (SP) 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations." This guide provides an overview of CM roles and responsibilities, a CM overview, the NIST SP 800-53 CM control requirements, per Federal Information Processing Standard (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems" security categorization level, and procedures and guidance for implementing these requirements.

Executive Order (EO) 13800, Presidential Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," requires all agencies to use "The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by NIST or any successor document to manage the agency's cybersecurity risk." This NIST document is commonly referred to as the Cybersecurity Framework (CSF). GSA uses the NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," commonly referred to as the Risk Management Framework (RMF) as its foundation for managing risk, assessment and authorization (A&A) of systems, and the implementation of NIST SP 800-53, Revision 5 controls. Further information on how CM controls relate to the CSF is provided in Appendix A.

Note: GSA is in the process of developing and updating CIO 2100.1 to align to the CSF 2.0, once that process is completed, the next version of this guide will align to it.

1.1 Purpose

The purpose of this guide is to provide guidance for the CM controls identified in NIST SP 800-53 and CM requirements specified in CIO 2100.1. This guide provides GSA Federal employees and contractors with significant security responsibilities (as identified in CIO 2100.1), and other IT personnel involved in the CM of IT assets, the specific procedures and processes they are to follow for configuration management of GSA systems under their purview.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in the configuration management of GSA systems and data. All GSA systems must adhere to the requirements and guidance provided with regards to the procedures, processes, and methods for configuration management of systems as described in this guide. Per CIO 2100.1, a GSA system is a system used or operated:

- by the GSA; or
- on behalf of the GSA by a contractor of GSA or by another organization.

1.3 Policy

Appendix B contains CIO 2100.1 policy statements regarding configuration management.

1.4 References

Appendix C provides links to references used throughout this guide.

1.5 Configuration Management Roles and Responsibilities

Appendix D provides a listing of the roles and responsibilities related to implementing configuration management at GSA.

2 Configuration Management Overview

Configuration management is used to control changes to hardware, software, and documentation of a system throughout its lifecycle. It assists in streamlining change management processes and prevents changes that could detrimentally affect the security posture of a system. CM is an element of the operational controls of a system and is interrelated with numerous other security disciplines such as project management, risk management, maintenance, and security assessment and authorization. An effective CM program requires:

- Configuration identification;
- Configuration baseline management;
- Change control processes, including security and/or change impact analyses;
- Configuration status accounting; and
- Configuration auditing.

An effective CM process provides a structured method for applying technical and administrative changes and monitors the results of changes throughout the life cycle. CM provides assurance that the system in operation is the correct version and ensures that all proposed changes are reviewed for security implications prior to implementation. Configuration changes can have

security implications as they may introduce or remove vulnerabilities. Changes require updates to system documentation to reflect the changes or modifications to the system. In addition, changes may trigger an update to the risk assessment, and systems that are significantly modified may need to be re-assessed and re-authorized. GSA follows the guidance in NIST 800-37, Revision 2, Appendix F when determining what qualifies as a significant change.

2.1 Configuration Management and Security in the GSA SLC

GSA Order CIO 2140.4, states:

> "This Order sets forth policy for planning and managing IT solutions developed for or operated by GSA. This policy has been developed to assure the Solutions Life Cycle (SLC) discipline used is consistent with SLC guiding principles, acquisition planning requirements, and capital planning and investment control requirements. The term SLC replaces the term Software Development Life Cycle (SDLC) which was used in the past."

The GSA SLC is divided into nine phases as listed on the GSA Solutions Life Cycle Guidance Handbook. The nine phases of the SLC and their relationship to the NIST RMF Steps are listed in Table 2-1. Details of each phase are available on the GSA Solutions Life Cycle Guidance Handbook. Security considerations, including configuration management, should be addressed as early as possible and throughout the SLC to cost-effectively implement the security features and controls needed to reduce risks during the operation and maintenance of systems.

Table 2-1. SLC Phase Relationship to RMF Steps

SLC Phase	RMF Steps
Phase 1 – Solution Concept Development Identifies a business need requiring IT as part of the solution.	Prepare
Phase 2 – Planning Clarifies the project's objectives and plans all of the activities necessary to implement it	Prepare Categorize
Phase 3 – Requirements Analysis Defines functional user requirements and delineates requirements in terms of data, solution performance, security, and maintainability.	Categorize Select
Phase 4 – Design The physical characteristics of the solution are designed during this phase.	Implement
Phase 5 – Development Deliverables from the design phase are produced.	Implement
Phase 6 – Integration and Testing The various components of the solution are integrated and systematically tested in a development environment.	Implement Assess
Phase 7 – Implementation The solution or system modifications are installed and operated in a production environment.	Implement Assess Authorize
Phase 8 – Operations and Maintenance Solution is monitored for continual performance in accordance with user requirements and needed solution modifications are made.	Monitor

SLC Phase	RMF Steps
Phase 9 – Disposition Activities ensure the orderly termination of the solution and preserve the vital information about the solution so that some or all of the information may be reactivated in the future, if necessary.	Monitor

Although the RMF steps in Table 2-1 are portrayed linearly with respect to the phases in the SLC, the actual implementation is iterative. For example, during the Monitor step, new vulnerabilities might be discovered which may require reassessing the original security control selection and additional controls selected to mitigate the new risks. The iterative nature of the RMF may require phases 3-7 to be completed multiple times during a system's lifetime.

3 Implementation Guidance for CM Controls

The GSA-defined parameter settings included in the control requirements are in blue, italicized text and offset by brackets in the control text. As stated in Section 1.2, Scope, the requirements outlined within this guide apply to all GSA systems and must be followed by all GSA Federal employees and contractors involved in the configuration management of GSA systems. The GSA implementation guidance stated for each control applies to personnel and/or the systems operated on behalf of GSA.

Table 3-1 identifies the designation of CM controls as Common, Hybrid, or System-Specific Controls for both Federal and Contractor systems. Effectively, common controls are provided by GSA at the enterprise level or by one of GSA's Major Information Systems (e.g., General Support System), system specific controls are implemented at the system level, and hybrid controls have shared responsibilities. CIO-IT Security-18-90 describes the GSA enterprise-wide common and hybrid controls and outlines the responsible parties for implementing them.

Table 3-1. Designation of CM Controls

System Type	Federal	Contractor
Common	CM-01, CM-02(07), CM-11	
Hybrid	CM-07(05), CM-08(02), CM-08(03), CM-08(06), CM-08(07)	CM-01
System-Specific	CM-02, CM-02(02), CM-02(03), CM-03, CM-03(01), CM-03(02), CM-03(04), CM-03(06), CM-04, CM-04(01), CM-04(02), CM-05, CM-05(01), CM-06, CM-06(01), CM-06(02), CM-07, CM-07(01), CM-07(02), CM-08, CM-08(01), CM-08(04), CM-09, CM-10, CM-12, CM-12(01)	CM-02, CM-02(02), CM-02(03), CM-02(07), CM-03, CM-03(01), CM-03(02), CM-03(04), CM-03(06), CM-04, CM-04(01), CM-04(02), CM-05, CM-05(01), CM-06, CM-06(01), CM-06(02), CM-07, CM-07(01), CM-07(02), CM-07(05), CM-08, CM-08(01), CM-08(02), CM-08(03), CM-08(04), CM-08(06), CM-08(07), CM-09, CM-10, CM-11, CM-12, CM-12(01)

Table 3-2 identifies GSA CM control applicability at the FIPS 199 Low, Moderate, and High levels.

Table 3-2. GSA Designation of CM Control Applicability

FIPS 199 Level	Applicable Controls
Low	CM-1, CM-02, CM-04, CM-05, CM-06, CM-07, CM-08, CM-10, CM-11
Moderate	CM-1, CM-02, CM-02(02), CM-02(03), CM-02(07), CM-03, CM-03(01)**, CM-03(02), CM-03(04), CM-04, CM-04(02), CM-05, CM-06, CM-06(01)*, CM-07, CM-07(01), CM-07(02), CM-07(05), CM-08, CM-08(01), CM-08(02)*, CM-08(03), CM-08(06)*, CM-08(07)**, CM-09, CM-10, CM-11, CM-12, CM-12(01)
High	CM-1, CM-02, CM-02(02), CM-02(03), CM-02(07), CM-03, CM-03(01), CM-03(02), CM-03(04), CM-03(06), CM-04, CM-04(01), CM-04(02), CM-05, CM-05(01), CM-06, CM-06(01), CM-06(02), CM-07, CM-07(01), CM-07(02), CM-07(05), CM-08, CM-08(01), CM-08(02), CM-08(03), CM-08(04), CM-08(06)*, CM-08(07)**, CM-09, CM-10, CM-11, CM-12, CM-12(01)
LATO	CM-02(02), CM-03(01), CM-07(05), CM-08(02),
MiSaaS	CM-02, CM-02(02), CM-03, CM-06, CM-06(01), CM-07(02), CM-08

*-control is applicable at the level listed per GSA OCISO tailoring
**-control is applicable at the level listed per GSA OCISO Tailored Moderate Baseline

For readers' ease of use, "mini tables" (see Table 3-3) that contain control/enhancement designation and applicability information are provided at the end of control statements for each CM control. The tables allow readers to see if a control/enhancement is applicable at their system's FIPS Level/A&A process and if it is common (C), Hybrid (H), or system specific (S), eliminating the need to refer back to Tables 3-1 and 3-2 for this information.

Table 3-3. Example Mini Table

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
Control ID	✓	✓	✓			C	H

3.1 CM-01 Policy and Procedures

Control:

a. Develop, document, and disseminate to [personnel with IT security responsibilities as defined in GSA CIO Order 2100.1]:
   1. [Organization-level] configuration management policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;
b. Designate an [CISO] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and
c. Review and update the current configuration management:
   1. Policy [annually, as part of CIO 2100.1 update] and following [changes to Federal or GSA policies, requirements, or guidance]; and
   2. Procedures [at least every three (3) years] and following [changes to Federal or GSA policies, requirements, or guidance].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-01	✓	✓	✓			C	H

Common Control Implementation:
The GSA configuration management policy is defined in the GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding configuration management of GSA systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency Directives Library website.

Configuration management procedures are documented in CIO-IT Security-01-05: Configuration Management (CM). The procedures facilitate the implementation of the configuration management policy and associated controls. This guide is disseminated GSA-wide via GSA's InSite centralized agency IT Security Procedural Guides website.

Per 2100.1, the Chief Information Security Officer (CISO) is responsible for managing the development and publishing of all security policies and IT security procedural guides.

The GSA OCISO is responsible for reviewing and updating:

1. CIO 2100.1 annually and following changes to Federal or GSA policies, requirements, or guidance.
2. CIO-IT Security-01-05 every three years and following changes to Federal or GSA policies, requirements, or guidance.

Federal System-Specific Expectation:
None, CM-01 is a common control.

Vendor/Contractor System-Specific Expectations: Vendors/contractors may defer to the GSA policy and guide or implement their own configuration management policies and procedures which comply with the GSA's requirements with the approval of the AO.

3.2 CM-02 Baseline Configuration

Control:

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and
b. Review and update the baseline configuration of the system:
   1. [Annually];
   2. When required due to [significant change as defined in NIST SP 800-37 Revision 2, Appendix F]; and
   3. When system components are installed or upgraded.

Control Enhancements:

(02) Baseline Configuration | Automation Support for Accuracy and Currency. Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [automated mechanisms as identified in the SSPP/CM Plan].

(03) Baseline Configuration | Retention of Previous Configurations. Retain [GSA SSO or Contractor recommended number of previous versions of baseline configurations of the system approved by the GSA CISO and AO] of previous versions of baseline configurations of the system to support rollback.

(07) Baseline Configuration | Configure systems and Components for High-Risk Areas.

(a) Issue [specially configured notebook computers with sanitized hard drives] with [limited applications, and additional hardening (e.g., more stringent configuration settings)] to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Apply the following controls to the systems or components when the individuals return from travel: [GSA standards (e.g., baseline configuration, system image, standard build configuration). Reference the GSA Enterprise Architecture Committee (EARC) Approved IT Standards at - https://ea.gsa.gov/#!/itstandards].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-02	✓	✓	✓		✓	S	S
CM-02(02)		✓	✓	✓	✓	S	S
CM-02(03)		✓	✓			S	S
CM-02(07)		✓	✓			C	S

Federal System Common-Control Implementation:
For CM-02(07), any GSA employee or contractor issued Government furnished equipment (GFE) who must work while overseas (with the exception of the OIG employees), shall be issued loaner devices by GSA IT when traveling outside the United States, or any area deemed to have an elevated risk during the period of travel.

The loaner devices must be returned to GSA IT immediately upon the employee's return. These loaner devices shall be wiped immediately by GSA IT to ensure no data remains resident on the system(s) issued. After wiping, the system will be configured in accordance with GSA standards.

System-Specific Expectations:
For CM-02, baseline configurations must be developed, documented, maintained, and sets of specifications for systems or configuration items within those systems (i.e., what is on a component) agreed upon. GSA Order 2100.1 and CIO-IT Security-06-30 require that system documentation be updated to reflect the current system configuration as specified by the control parameters. The baseline configurations serve as a basis for future builds, releases, and/or changes to systems and components. The following bullets present implementation guidance for documenting the system's configuration baseline:

- Ensure the system's configuration baseline is based on GSA standards. Visit the GSA's IT Standards website for approved standards or to identify products or technical standards approved for current production deployment. The standards are consistent with GSA's enterprise architecture.
- Develop a system baseline configuration that is consistent with GSA's enterprise architecture. Include how the system is linked to the GSA mission.

Baseline configurations must be reviewed and updated at least annually, and when significant changes occur per the control parameter or when components are installed or upgraded.

For CM-02(02), GSA leverages existing enterprise security and CDM tools including BigFix and Tenable to maintain, manage, and verify baseline configurations. Integration with these tools and capabilities can assist systems in satisfying this control.

For CM-02(03), GSA systems must maintain the previous version of the system's baseline configurations to support rollback capabilities.

Vendor/Contractor System-Specific Expectations:
For CM-02 and CM-02(03) vendors/contractors may defer to the GSA configuration standards as specified above or implement their own system baseline configuration which complies with GSA's requirements with the approval of the GSA CISO and AO.

For CM-02(02), vendors/contractors must use automated mechanisms similar to the GSA tools identified above and as documented in the System's Security and Privacy Plan (SSPP)/Configuration Management (CM) Plan.

For CM-02(07), vendors/contractors must have a process for addressing systems or system components that are taken to high-risk areas and when they are returned. The process must be documented in the system's SSPP.

3.3 CM-03 Configuration Change Control

Control:

a. Determine and document the types of changes to the system that are configuration-controlled;
b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
c. Document configuration change decisions associated with the system;
d. Implement approved configuration-controlled changes to the system;
e. Retain records of configuration-controlled changes to the system for [as long as deemed necessary by GSA SSO or Contractor and approved by the GSA CISO and AO];
f. Monitor and review activities associated with configuration-controlled changes to the system; and
g. Coordinate and provide oversight for configuration change control activities through [a defined CM approval process (example: a charted Configuration Change Board (CCB))] that convenes [on a defined basis in support of the system's CM requirements to approve changes such as:
- Upgrades and modifications to the information system or its components
- Changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers)
- Emergency changes required to address an immediate issue
- Changes to remediate flaws].

Control Enhancements:

(01) Configuration Change Control | Automated Document, Notification, and Prohibition of Changes. Use [automated mechanisms as identified in the SSPP/CM Plan] to:
  (a) Document proposed changes to the system;
  (b) Notify [GSA SSO or Contractor recommended approval authorities approved by the GSA CISO and AO] 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 [GSA SSO or Contractor recommended time period approved by the GSA CISO and AO];
(d) Prohibit changes to the system until designated approvals are received;
(e) Document all changes to the system; and
(f) Notify [Administrators (Application, System, Network, etc.), ISSO, ISSM, System Owner] when approved changes to the system are completed.

(02) Configuration Change Control | Test, Validate, and Documentation of Changes. Test, validate, and document changes to the system before finalizing the implementation of the changes.

(04) Configuration Change Control | Security and Privacy Representatives. Require [security and privacy representatives as defined in the SSPP/CM Plan] to be members of the [defined configuration change control element (e.g., a charted Configuration Change Board (CCB))].

(06) Configuration Change Control | Cryptography Management. Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [AU-9(3), CP-9(8), IA-7, SC-8(1), SC-12, SC-13, SC-28(1)].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-03		✓	✓		✓	S	S
CM-03(01)		✓**	✓	✓		S	S
CM-03(02)		✓	✓			S	S
CM-03(04)		✓	✓			S	S
CM-03(06)			✓			S	S

**-control is applicable at the level listed per GSA OCISO Tailored Moderate Baseline

System-Specific Expectations:
Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. This control focuses on defining the CM process, controlling the system configuration according to that process, and ensuring that no configuration changes are made without going through the approved change control process. Below are some general guidelines which can be included in the CM Plan template available on the GSA IT Security Forms and Aids webpage.

- Manage configuration changes to the system through a defined CM process (e.g., a charted CCB that approves proposed changes to the system. The defined CM process should monitor the following:
  - Changes to the system, including upgrades, modifications, and maintenance changes
  - Changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers).
  - Emergency changes
  - Changes to remediate flaws.
- Authorize, document, and control changes to the system. Include emergency changes in the configuration change control process.

- Conduct an impact analysis (per CM-04) to determine the ramifications of the proposed change. Consider changes only after analyzing the results of the security impact analysis.
- Use automated tools/processes to control/manage system changes (e.g., ServiceNow). If automated tools are not used, a GSA Change Request Form is available on the GSA IT Security Forms and Aids page.
- Document all approved configuration-controlled changes in appropriate documentation. The current state of the system should be the 'as-built' configuration as reflected in the initial baseline with approved changes.
- Audit activities associated with configuration changes to the system. Review the approved configuration management process for key auditable activities and then review records of selected activities in the process, for example:
  - Who approved the change request;
  - Who implemented the change;
  - Who completed the security impact assessment;
  - Who tested the change; and
  - How it was tested.
- Ensure that any testing performed does not adversely impact the system (perform the test on a test platform, not a production platform).
- Per NARA General Records Schedule 3.1 records created for configuration and change management must be retained for 5 years but may be retained for longer if required based on business use.

For CM-03(01), systems are required to use automated tools to document proposed changes and notify when changes are approved and implemented. GSA uses a number of tools to manage changes (e.g., ServiceNow) or prevent changes (e.g., Bit9) to systems. The specific tools used must be documented in the SSPP and configuration management plans.

For CM-03(02), systems are required to test, validate, and document changes before implementation in the operational environment.

For CM-03(04), systems are required to have security and privacy representatives as identified in the system's SSPP and configuration management plan to be members of the defined configuration change control element.

For enhancement CM-03(06), systems are required to ensure that the following controls used for cryptographic mechanisms are under configuration management: AU-09(03), CP-09(08), IA-07, SC-08(01), SC-12, SC-13, SC-28(01).

3.4 CM-04 Impact Analysis

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

Control Enhancement:

(01) Impact Analysis | Separate Test Environments. 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.

(02) Impact Analysis | Verification of Controls. After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-04	✓	✓	✓			S	S
CM-04(01)			✓			S	S
CM-04(02)		✓	✓			S	S

System-Specific Expectations:
For CM-04, conduct impact analyses prior to implementing any changes (including patches, upgrades, and modifications) to the system and checking the system after changes have been implemented for unintended consequences. Below are some general guidelines:

- Employ measures for documenting and monitoring changes to the system in the SSPP or CM plan.
- Analyze changes to the system to determine potential security impacts prior to change implementation and as part of the change approval process.
- Use GSA's Security Impact Analysis Form to perform impact analyses. Impact analyses must follow the following guidelines:
  - Be conducted by personnel with the proper information security responsibilities.
  - Be performed by individuals with the appropriate skills and technical expertise to analyze the changes to systems and the associated security ramifications.
  - Include:
    - Reviewing system documentation such as the SSPP to understand how specific security controls are implemented within the system and how the changes might affect the controls.
    - Assessing risk to understand the impact of the changes and to determine if additional security controls are required.
  - Scale the impact analysis in accordance with the impact level of the system.
  - Verify system security features are still functioning properly after the system is changed (including upgrades and modifications).

For CM-04(01), systems must analyze changes in a separate test environment before implementation in an operational environment.

For CM-04(02), systems must verify that any controls impacted by the changes are still implemented correctly, operating as intended, and producing the desired outcome.

3.5 CM-05 Access Restrictions for Change

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

Control Enhancements:

(01) Access Restrictions for Change | Automated Access Enforcement and Audit Records.

a. Enforce access restrictions using [automated mechanisms as documented in the SSPP/CM Plan]; and
b. Automatically generate audit records of the enforcement actions.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-05	✓	✓	✓			S	S
CM-05(01)	✓	✓	✓			S	S

System-Specific Expectations:
For CM-05, only qualified and authorized individuals should be allowed access for initiating changes, including upgrades and modifications. Examples of access restrictions include physical and logical access controls (see AC-03 and PE-03), workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover). Ensure there is a process in place to approve and enforce:

- Individual access privileges to systems;
- Physical and logical access restrictions associated with changes to the system;
- System upgrades; and
- System modifications.

For CM-05(01), systems must implement automated processes to restrict and audit changes and document them in the system's SSPP/CM Plan.

3.6 CM-06 Configuration Settings

Control:

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as reviewed and accepted by the GSA CISO and AO];
b. Implement the configuration settings;
c. Identify, document, and approve any deviations from established configuration settings for [all components] based on [explicit operational requirements]; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Control Enhancements:

(01) Configuration Settings | Automated Management, Application, and Verification. Manage, apply, and verify configuration settings for [all operating systems] using [automated mechanisms as documented in the SSPP/CM Plan].
(02) Configuration Settings | Respond to Unauthorized Changes. Take the following actions in response to unauthorized changes to [configuration settings as specified in CM-6a]: [investigate how the unauthorized changes occurred and apply remediation actions to reconfigure the system and keep similar changes from occurring].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-06	✓	✓	✓		✓	S	S

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-06(01)		✓*	✓	✓	✓	S	S
CM-06(02)			✓			S	S

*-control is applicable at the level listed per GSA OCISO tailoring

System-Specific Expectations:
For CM-06, System Owners are responsible for configuring systems in agreement with GSA technical guidelines/benchmarks. GSA benchmarks may be exceeded but not lowered. If no technical guideline/benchmark is available for a particular technology, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines may be used, as accepted by the GSA CISO and AO. Configure the security settings to the most restrictive mode consistent with operational requirements in all components of the system. GSA CIO-IT Security Technical Guides and Standards are available on the IT Security Technical Guides and Standards page.

Security settings that are not completely implemented because of operational requirements should be documented in the SSPP. Any deviations, not following GSA policies and standards must be submitted using the Security Deviation Request Google Form. The system owner must monitor and control changes in accordance with the system's CM Plan, CM processes, and GSA policies and procedures. GSA's ISO Division scans for configuration compliance on a regular basis and provides the data to the appropriate system POC for review and resolution, as necessary.

When submitting security deviation requests to GSA hardening guidelines/benchmarks System Owners must observe the following:

- Any baseline hardening deviations must be coordinated by the ISSO/ISSM.
- Deviations to CIS Level 1 and Level 3 (Defense Information Security Agency [DISA] Security Technical Implementation Guide [STIG]) settings require AO approval.
- Deviations to CIS Level 2 settings can be reviewed and concurred to by the ISSM.

Federal System-Specific Expectations:
For enhancements CM-06(01) and 6(02), GSA uses automated tools such as FireEyeHX and BigFix to verify configuration settings and provides reports on differences (changes) so appropriate system personnel can investigate if unauthorized changes have been made.

Vendor/Contractor System-Specific Expectations:
For enhancements CM-06(01) and 6(02), the vendor/contractor is responsible for using automated tools to manage, apply, and verify configuration settings and provide information on differences (changes) so appropriate system personnel can investigate if unauthorized changes have been made.

3.7 CM-07 Least Functionality

Control:

a. Configure the system to provide only [mission essential capabilities in accordance with the Business Impact Analysis (BIA)]; and
b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [as specified in GSA technical guidelines, NIST guidelines, Center for Internet

Security guidelines, or industry best practice guidelines, as deemed appropriate by the GSA CISO and AO].

Control Enhancements:

(01) Least Functionality | Periodic Review.
  (a) Review the system [annually as part of SSPP update] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and
  (b) Disable or remove [GSA SSO or Contractor recommended functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure as approved by the GSA CISO and AO].

(02) Least Functionality | Prevent Program Execution. Prevent program execution in accordance with [CIO 2100.1 policies and GSA SSO or Contractor recommended list of authorized software programs, a list of unauthorized software programs, and rules authorizing the terms and conditions of software program usage, as approved by the GSA CISO and AO].

(05) Least Functionality | Authorized Software – Allow-By-Exception.
  (a) Identify [GSA SSO or Contractor recommended software programs authorized to execute on the information system as approved by the GSA CISO and AO];
  (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 [annually as part of SSPP update].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-07		✓	✓	✓		S	S
CM-07(01)		✓	✓			S	S
CM-07(02)		✓	✓		✓	S	S
CM-07(05)		✓	✓	✓		H	S

Common Control Implementation:
For CM-07(05), the GSA uses Carbon Black (Bit9) for Windows systems to:

- permit authorized software to execute; and
- deny unauthorized software from executing.

Details on the common control implementation of Carbon Black (Bit9) are available in the SecTools SSPP and CRM.

For non-Windows systems ISSOs/ISSMs/System Owners should contact GSA's Security Operations Division (ISO) regarding the use of Carbon Black or other mechanisms/methods.

The GSA ISO Division is responsible for updating the list of authorized software programs in Carbon Black (Bit9).

System-Specific Expectations:
For CM-07, the system and each of its components should provide only the functions required to accomplish their missions. Where feasible, component functionality should be limited to a single function per device (e.g., database server or web server, not both).

Permitted or allowed functions, ports, protocols, and/or services should be specifically defined in the system's SSPP, all others should be prohibited or restricted. Technical security configurations are documented in the hardening guides used by the system, i.e., GSA, NIST, Center for Internet Security, or industry best practice guidelines as deemed appropriate by the GSA CISO and AO.

For enhancements CM-07(01) and 07(02) systems must:

- Conduct an annual review of the functions, ports, protocols, and services provided and disable any that are not approved or are unnecessary.
- Prevent programs from executing that are listed as unauthorized, not listed as authorized, or are not allowed based on the rules, terms, and conditions approved by the GSA CISO and AO.
- Use allow-by-exception capabilities to deny unauthorized software and allow authorized software to execute on the system. GSA uses automated tools such as Carbon Black (Bit9) to support allow-by-exception. ISSOs/ISSMs/System Owners should coordinate with GSA's ISO Division if Carbon Black is not suitable for a specific system.
- Systems must review and update the list of authorized software programs as part of their annual SSPP update.

Vendor/Contractor System-Specific Expectations:
For CM-07, CM-07(01), and CM-05(02), follow the system-specific guidance above. For CM-07(05), vendors/contractors must identify the software programs allowed to execute on the system and establish a policy enforcement mechanism that only allows the allowed software to execute and review the list of authorized software annually.

3.8 CM-08 System Component Inventory

Control:

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: [GSA SSO or Contractor recommended information deemed necessary to ensure property accountability as approved by the GSA CISO and AO. List may include hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address]; and

b. Review and update the system component inventory [monthly].

Control Enhancements:

(01) System Component Inventory | Updates During Installation and Removal. Update the inventory of system components as part of component installations, removals, and system updates.

(02) System Component Inventory | Automated Maintenance. Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [automated mechanisms as documented in the SSPP/CM Plan].

(03) System Component Inventory | Automated Unauthorized Component Detection.
(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [automated mechanisms as documented in the SSPP/CM Plan] [on an ongoing basis]; and
(b) Take the following actions when unauthorized components are detected: [isolates the components and notifies GSA SSO or Contractor recommended and GSA approved personnel or roles]

(04) System Component Inventory | Accountability Information. Include in the system component inventory information, a means for identifying by [name, position, and role], individuals responsible and accountable for administering those components.

(06) System Component Inventory | Assessed Configurations and Approved Deviations. Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.

(07) System Component Inventory | Centralized Repository. Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-08	✓	✓	✓		✓	S	S
CM-08(01)		✓	✓			S	S
CM-08(02)		✓*	✓	✓		H	S
CM-08(03)		✓	✓			H	S
CM-08(04)			✓			S	S
CM-08(06)		✓*	✓*			H	S
CM-08(07)		✓**	✓**			H	S

*-control is applicable at the level listed per GSA OCISO tailoring
**-control is applicable at the level listed per GSA OCISO Tailored Moderate Baseline

Federal Systems Common Control Implementation:
For CM-08(02), CM-08(03), CM-08(06), CM-08(07)**,** GSA uses automated tools (e.g., ServiceNow, Tenable Security Center, ForeScout/Secure Connector, BigFix) to assist in maintaining system inventories. The inventory must provide coverage for all assets in the system inventory including physical servers and virtual servers or virtual machines, workstations, mobile devices, and network devices (as applicable). Any information determined to be necessary to achieve effective accountability should be included. GSA requires inventories to be reviewed and updated monthly to ensure vulnerability scanning is performed on all system assets. As GSA continues to implement its Continuous Diagnostics and Mitigation (CDM) tools they will be key in having up to date inventories.

GSA employs automated tools (e.g., Carbon Black (Bit9), BigFix, Forescout, Tenable Nessus) and GSA's Governance, Risk and Compliance (GRC) tool to maintain inventory tracking. If any duplicate systems are identified (an inventory item in more than one authorization boundary) the system owners are contacted to resolve the duplication. Details on the common control implementation are available in the SecTools SSPP.

For CM-08(02), GSA also uses BigFix, MaaS360, and Google MDM for client and mobile device inventory, and HP Web JetAdmin for printer inventory.

For CM-08(03), GSA employs automated tools (e.g., Carbon Black (Bit9), Cylance, FireEyeHX) to detect unauthorized components on an ongoing basis. Details on the common control

implementation are available in the SecTools SSPP. GSA isolates any unauthorized components and notifies appropriate personnel. Details on the common control implementation are available in the SecTools SSPP.

For CM-08(06), the system inventory as stated above is documented in Section 10 of the SSPP, and assessed components are identified in the Security Assessment Plan and Report of the system. Any deviations to configurations must be submitted using the Security Deviation Request Google Form.

For CM-08(07), GSA's Enterprise Operations Program uses ServiceNow for a centralized inventory of system components.

Federal System-Specific Expectations:
For CM-08, The system component inventory is defined in Section 10 of the system's SSPP, System Environment. Systems must maintain an up-to-date component inventory. Include any information determined to be necessary to achieve effective accountability, including the appropriate level of granularity for inventory items. The granularity and type of information will often be different for physical versus virtual components. However, inventory information may include:

- IP address
- Host name
- OS version
- Application version
- Hardware specifications, including:
  - Manufacturer
  - Type
  - Model
  - Serial number
  - Physical location
- Software license information
- system/component owner
- Machine name and network address (if a network device).

In addition, System Owners, ISSOs, and ISSMs must ensure the GSA tools are deployed on their systems and they are integrated with the GSA security stack. Details on the specific control implementations are available in the SecTools SSPP. For systems not integrated with the GSA security stack, this control is system specific and tools with similar capabilities to SecTool's tools must support the control requirements.

For CM-08(01), CM-08(02), CM-08(03), CM-08(06) and CM-08(07) systems must:

- Update the inventory during installations, removals, and system updates (i.e., not just monthly).
- Use the GSA automated tools identified in the control implementation details to maintain the inventory.
- Use the same GSA automated tools or other automated tools to detect unauthorized components, and if found isolate the components and notify the appropriate personnel (i.e., ISSO/ISSM, System Owner, Custodians).
- Use the same GSA automated tools to ensure components are not duplicated across system inventories.

- Include the “as-is” state of components (i.e., assessed configurations and approved deviations) in the inventory and document deviations as described earlier.

For CM-08(04) systems must include in the inventory the name, position, and role of the administrator of the component.

Vendor/Contractor System-Specific Expectations:
For CM-08, CM-08(01), CM-08(02), CM-08(03), CM-08(04), CM-08(06) and CM-08(07), vendors/contractors must implement the control similar to the manner for Federal systems as described above, and with vendor/contractor’s tools providing similar automated capabilities as GSA’s tools.

3.9 CM-09 Configuration Management Plan

Control: 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 [defined CM personnel (e.g., charted Configuration Change Board (CCB))]; and
e. Protects the configuration management plan from unauthorized disclosure and modification.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-09		✓	✓			S	S

System-Specific Expectations:
System owners must ensure the system’s CM Plan addresses:

- Roles and responsibilities for CM of the system.
- Identification of the Configuration Items (CIs) to be placed under CM for the system.
- CM processes and procedures used to manage the system’s baseline.
- How change control is managed and communicated.
- How configuration status accounting and auditing is maintained.
- How CM is managed throughout a systems life cycle.
- Review and approval by the CM personnel identified in the CM plan.

Note: Security must be addressed throughout the CM Plan and process. This is primarily established by conducting security impact analyses (see CM-04) when changes are proposed and ensuring changes are effectively controlled.

A Configuration Management Plan Template is available on the GSA IT Security Forms and Aids page.

3.10 CM-10 Software Usage Restrictions

Control:

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.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-10	✓	✓	✓			S	S

Federal System-Specific Expectations:
Systems must adhere to GSA contracts, copyright laws, and licensing agreements. The GSA uses standard configurations for workstations and servers to establish the authorized/approved software for systems. Users are required to request software through ServiceNow which is also GSA's Software License Management Repository as described in GSA CIO Order 2108.1, "CIO Software License Management." In accordance with CIO Order 2100.1, peer-to-peer networking technologies are prohibited on GSA systems and networks except if approved by the OCISO. GSA uses Carbon Black (Bit9) to prohibit installation of such technologies.

Vendor/Contractor System-Specific Expectations:
Vendors/contractors systems must adhere to their contracts, copyright laws, and licensing agreements. The systems must also comply with CIO Order 2100.1 regarding peer-to-peer networking.

3.11 CM-11 User-Installed Software

Control:

a. Establish [policies as specified in CIO 2100.1] governing the installation of software by users;
b. Enforce software installation policies through the following methods: [automated methods (i.e., configuration/compliance scans)]; and
c. Monitor policy compliance [on an ongoing basis].

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-11	✓	✓	✓			C	S

Common Control Implementation:
CIO 2100.1 and the GSA IT Rules of Behavior for General Users state that users can only use authorized software from GSA or GSA approved sources and must not install any software without approval through the IT standards process.

GSA uses Carbon Black (Bit9) to prohibit users from installing unauthorized software. Details on the common control implementation are available in the SecTools SSPP.

GSA uses Carbon Black (Bit9) to monitor users and prohibit the installation of unauthorized software. Details on the common control implementation are available in the SecTools SSPP.

Federal System-Specific Expectations:
None, common control.

Vendor/Contractor System-Specific Expectations: Vendors/contractor systems may adhere to GSA policies regarding the installation of software or have their own policies that meet the control requirements. Vendors/contractors must enforce the policies and monitor compliance with the policies using tools with similar functions as described above.

3.12 CM-12 Information Location

Control:

a. Identify and document the location of [Personally Identifiable Information (PII); Payment Card Industry (PCI) data; Identity, Credentialing, and Access Management (ICAM) data (includes but is not limited to identifier and authenticator data such as passwords, tokens, keys, certificates, hashes); system- and application-security log data; and, other sensitive data as determined by the GSA CISO and AO] 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.

Control Enhancements:

(01) Information Location | Automated Tools to Support Information Location. Use automated tools to identify [Personally Identifiable Information (PII); Payment Card Industry (PCI) data; Identity, Credentialing, and Access Management (ICAM) data (includes but is not limited to identifier and authenticator data such as passwords, tokens, keys, certificates, hashes); system- and application-security log data; and, other sensitive data as determined by the AO] on [all system components for external information systems] to ensure controls are in place to protect organizational information and individual privacy.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
CM-12		✓	✓			S	S
CM-12(01)		✓	✓			S	S

System-Specific Expectations:
As part of developing the system SSPP, and completing a FIPS PUB 199 categorization, and Privacy Threshold Assessment/Privacy Impact Assessment, systems must document the location and components containing PII, PCI, ICAM, security log, and other sensitive data. In the SSPP the system users, roles, and privileges allowing access to the sensitive data must be documented. At a minimum, systems must update their SSPPs on an annual basis, including any changes regarding the system, its components, data, user's access to sensitive data, and its location.

Systems must use automated tools (e.g., firewalls, Data Layer Protection devices) to identify the specified information on all components of external information systems in order to ensure that any necessary controls (e.g., encryption, access controls) are in place to protect the sensitive data.

4 Appendix A: CSF Categories/Subcategories

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's RMF as its primary risk management process. Table A-1 lists the Categories and Subcategories from the CSF that are identified as related to the implementation of policies, procedures, and processes implementing the NIST SP 800-53, Revision 5 AC controls. CIO 2100.1 and this procedural guide provide GSA's policies and procedural guidance regarding access control to GSA systems and implementing CM controls.

Table A-1. CSF Categories/Subcategories and the CM Control Family

CSF Category/ Subcategory Identifier	Definition/Description
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried. (CM-08) **ID.AM-2:** Software platforms and applications within the organization are inventoried. (CM-08)
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated. (CM-01) **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. (CM-01)
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-5:** Assets are formally managed throughout removal, transfers, and disposition. (CM-08 **PR.DS-7:** The development and testing environment(s) are separate from the production environment. (CM-02)
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality). (CM-02, CM-03, CM-04, CM-5, CM-06, CM-07, CM-09) **PR.IP-3**: Configuration change control processes are in place. (CM-03, CM-04)
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities (CM-07)
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed (CM-02)
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events (CM-10, CM-11)

5 Appendix B: Policy

The following extracts from CIO 2100.1 contain information related to configuration management of GSA systems.

Chapter 3: Policy for Identify Function

1. Asset management.

a. System Owners and their teams, ISSMs, and ISSOs must maintain the following inventories in coordination with the OCISO:

(1) An inventory of GSA information systems (including hardware, software, and other data required by Federal or GSA requirements) in GSA's official system inventory repository;
(2) An inventory of the devices/components comprising information systems IAW GSA CIO-IT Security-01-05, Configuration Management (CM);

Chapter 4: Policy for Protect Function

5. Information Protection Processes and Procedures.

a. All information systems must be securely configured IAW with GSA IT technical guides and standards, updated, and patched before being put into operation and while in operation.

b. GSA information systems, including vendor owned/operated systems on behalf of GSA, must configure their systems in agreement with GSA technical guidelines, NIST guidelines, DISA STIG guidelines (High Severity/CAT I), Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate. Any GSA security benchmark published for a particular technology must be referenced to securely configure that technology. GSA security benchmark requirements must be implemented within (180) days of the benchmark's publication. GSA benchmarks may be exceeded but not lowered.

h. Configuration changes must be controlled IAW the security controls and processes described in GSA CIO-IT Security-01-05.

7. Protective Technology.

k. Information systems must be configured to the most restrictive mode (e.g., limiting ports, protocols, services, etc.) consistent with operational requirements.

6 Appendix C: References

Federal Laws, Standards, Regulations, and Publications:

- EO 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- National Archives and Records Administration (NARA) General Records Schedule 3.1: General Technology Management Records
- NIST CSF, Framework for Improving Critical Infrastructure Cybersecurity
- NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations

GSA Policies, Procedures, Guidance:

- GSA Order CIO 2100.1, GSA Information Technology (IT) Security Policy
- GSA Order CIO 2108.2, CIO Software License Management
- GSA Order CIO 2140.4, Information Technology (IT) Solutions Life Cycle (SLC) Policy

The GSA CIO-IT Security Procedural Guides listed below are available on the IT Security Procedural Guides page.

- CIO-IT Security-06-30, Managing Enterprise Cybersecurity Risk
- CIO-IT Security-18-90, Common Control Catalog (CCC)

GSA Templates and Forms:

The following templates/forms supporting configuration management are available on the GSA IT Security Forms and Aids page.

- Change Request Form - for GSA systems that do not use an automated tool (e.g., ServiceNow, JIRA) for configuration management.
- Configuration Management Plan Template

7 Appendix D: Roles and Responsibilities

There are many roles associated with implementing an effective configuration management process for systems. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. The responsibilities listed in this guide are focused on implementing configuration management with a security focus for systems. A complete set of GSA security roles and responsibilities can be found in CIO 2100.1.

Authorizing Official (AO)

Responsibilities include the following:

- Ensuring that GSA information systems under their purview have implemented the required CM controls in accordance with GSA and Federal policies and requirements.
- Identifying the level of acceptable risk for an information system and determining whether an acceptable level of risk has been obtained, including risks associated with CM controls.
- Ensuring all information systems, applications, or sets of common controls under their purview have a current ATO issued per GSA CIO-IT Security-06-30.
- Ensuring a plan of action and milestones (POA&M) entry is developed and managed to address any CM controls that are not fully implemented.

Information System Security Manager (ISSM)

Responsibilities include the following:

- Assisting ISSOs, as necessary, to ensure NIST SP 800-53 CM controls are in place and operating as intended.
- Verifying systems under their purview have appropriately addressed NIST SP 800-53 CM controls.
- Coordinating with the AO, System Owner, ISSOs, and OCISO Directors, as necessary, regarding CM control implementation and compliance with NIST and GSA requirements.
- Working with the ISSO and System Owner to develop and manage POA&Ms regarding CM controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.

Information System Security Officer (ISSO)

Responsibilities include the following:

- Ensuring necessary CM controls are in place and operating as intended.
- Coordinating with ISSMs and System Owners, as necessary, regarding CM control implementation and compliance with NIST and GSA requirements.
- Working with the System Owner and ISSM to develop and manage POA&Ms regarding CM controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.

System Owners

Responsibilities include the following:

- Ensuring necessary NIST SP 800-53 CM controls are in place and operating as intended.
- Coordinating with ISSOs and ISSMs, as necessary, regarding CM control implementation and compliance with NIST and GSA requirements.
- Working with ISSOs and ISSMs to develop and manage POA&Ms regarding NIST SP 800-53 CM controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.
- Obtaining the resources necessary to securely implement and manage CM controls for their respective systems.
- Ensuring that for each system, CM is integrated into the solutions life cycle (SLC) from the information system's initiation phase to the system's disposal phase.

Data Owners/Functional Business Line Managers/Custodians

Responsibilities include the following:

- Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of CM control requirements, as necessary.
- Participating in the CM of systems as specified in CM Plans.