## VERSION HISTORY/CHANGE RECORD

### Revision 1 – July 13, 2005

<table>
<thead>
<tr>
<th>Change Number</th>
<th>Person Posting Change</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Page Number of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Heard/Scott</td>
<td>Changes made throughout the document to reflect FISMA, NIST and GSA Order CIO 2100.1B requirements.</td>
<td>Updated to reflect and implement various FISMA, NIST and GSA Order CIO 2100.1B requirements.</td>
<td>Various</td>
</tr>
<tr>
<td>2</td>
<td>Heard/Scott</td>
<td>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.</td>
<td>Updated to reflect the correlation of the CIO-IT Security Guides; and to further express policy within them as standalone documents.</td>
<td>Various</td>
</tr>
</tbody>
</table>

### Revision 2 – March 22, 2010

<table>
<thead>
<tr>
<th>Change Number</th>
<th>Person Posting Change</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Page Number of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Berlas/Wood</td>
<td>Changes made throughout the document to reflect NIST SP 800-53 R3 and GSA requirements.</td>
<td>Updated to reflect and implement NIST SP 800-53 R3 and GSA requirements.</td>
<td>Various</td>
</tr>
</tbody>
</table>

### Revision 3 – July 14, 2015

<table>
<thead>
<tr>
<th>Change Number</th>
<th>Person Posting Change</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Page Number of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Riaz/Searcy</td>
<td>Changes made throughout the document to reflect NIST and GSA requirements.</td>
<td>Updated to reflect and implement the most current NIST SP 800-53 and GSA requirements.</td>
<td>Various</td>
</tr>
</tbody>
</table>

### Revision 4 –

<table>
<thead>
<tr>
<th>Change Number</th>
<th>Person Posting Change</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Page Number of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Feliksa/Klemens</td>
<td>Changes made throughout the document to reflect NIST and GSA requirements.</td>
<td>Updated to reflect GSA’s current development and configuration management processes. Updated to align with Federal, NIST, and GSA guidance.</td>
<td>Throughout</td>
</tr>
</tbody>
</table>
Approval

IT Security Procedural Guide: Configuration Management (CM), CIO-IT Security-01-05, Revision 4, is hereby approved for distribution.

1/18/2018

Kurt Garbars
CISO
Signed by: KURT GARBARS

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

1 Introduction ...................................................................................................................... 1
  1.1 Purpose ..................................................................................................................... 2
  1.2 Scope ......................................................................................................................... 2
  1.3 Policy ........................................................................................................................ 3
  1.4 References ................................................................................................................ 3

2 Roles and Responsibilities .............................................................................................. 3
  2.1 Chief Information Security Officer (CISO) ................................................................. 4
  2.2 Authorizing Official (AO) ......................................................................................... 4
  2.3 Information System Security Manager (ISSM) .......................................................... 4
  2.4 Information System Security Officer (ISSO) ............................................................. 4
  2.5 System Owners (e.g., System Program Managers/Project Managers) ...................... 5
  2.6 Data Owners/Functional Business Line Managers/Custodians .................................. 5

3 Configuration Management Overview ............................................................................ 5
  3.1 Configuration Management and Security in the GSA SLC ......................................... 6

4 Implementation Guidance for CM Controls ................................................................. 7
  4.1 CM-1 Configuration Management Policy and Procedures ........................................ 7
  4.2 CM-2 Baseline Configuration ................................................................................... 8
  4.3 CM-3 Configuration Change Control ....................................................................... 10
  4.4 CM-4 Security Impact Analysis ............................................................................... 12
  4.5 CM-5 Access Restrictions for Change ..................................................................... 13
  4.6 CM-6 Configuration Settings ................................................................................... 14
  4.7 CM-7 Least Functionality ......................................................................................... 15
  4.8 CM-8 Information System Component Inventory ....................................................... 17
  4.9 CM-9 Configuration Management Plan .................................................................... 19
  4.10 CM-10 Software Usage Restrictions ....................................................................... 20
  4.11 CM-11 User-Installed Software .............................................................................. 21

5 Summary .......................................................................................................................... 21

Appendix A - Change Request Form .................................................................................. 23
Appendix B – Configuration Management Plan Template ................................................. 24
1 Introduction

Information 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 information 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 systems maintenance will be performed in a cost-effective or timely manner.

Every General Services Administration (GSA) Information Technology (IT) system 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 Systems Security Officer (ISSO) through the appropriate Information Systems 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 4, “Security and Privacy Controls for Federal Information Systems and Organizations”. This guide provides an overview of CM, roles and responsibilities, NIST SP 800-53 audit and accountability requirements per Federal Information Processing Standard (FIPS) 199, “Standards for Security Categorization of Federal Information and Information Systems”, security categorization level, and procedures for implementing these requirements.

Executive Order (EO), 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 the National Institute of Standards and Technology (NIST) or any successor document to manage the agency’s cybersecurity risk.” This NIST document is commonly referred to as the Cybersecurity Framework (CSF).

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), Recover (RC). The CSF complements, and does not replace, an organization’s risk management process and cybersecurity program. GSA uses NIST’s Risk Management Framework from NIST SP 800-37, Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach”. Table 1-1, NIST SP 800-53 Control to CSF Mapping, provides how the NIST SP 800-53 controls within this guide are aligned with the CSF Category Unique Identifiers. The following CSF categories are aligned with NIST’s CM controls.

- Identify-Governance (ID.GV)
- Identify-Asset Management (ID.AM)
- Protect-Data Security (PR.DS)
- Protect-Information Protection Processes and Procedures (PR.IP)
- Protect-Protective Technology (PR.PT)
- Detect-Anomalies and Events (DE.AE)
- Detect-Security Continuous Monitoring (DE.CM)

<table>
<thead>
<tr>
<th>NIST SP 800-53 Controls</th>
<th>CSF Category Unique Identifier Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-1</td>
<td>ID.GV-1, ID.GV-3</td>
</tr>
<tr>
<td>CM-2</td>
<td>PR.DS-7, PR.IP-1, DE.AE-1</td>
</tr>
<tr>
<td>CM-3</td>
<td>PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7</td>
</tr>
<tr>
<td>CM-4</td>
<td>PR.IP-1, PR.IP-3</td>
</tr>
<tr>
<td>CM-5</td>
<td>PR.IP-1</td>
</tr>
<tr>
<td>CM-6</td>
<td>PR.IP-1</td>
</tr>
<tr>
<td>CM-7</td>
<td>PR.IP-1, PR.PT-3</td>
</tr>
<tr>
<td>CM-8</td>
<td>ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7</td>
</tr>
<tr>
<td>CM-9</td>
<td>PR.IP-1</td>
</tr>
<tr>
<td>CM-10</td>
<td>DE.CM-3</td>
</tr>
<tr>
<td>CM-11</td>
<td>DE.CM-3</td>
</tr>
</tbody>
</table>

1.1 Purpose

The purpose of this guide is to provide guidance for the CM security controls identified in NIST SP 800-53 and CM requirements specified in CIO 2100.1. This procedural 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 maintaining GSA information 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 CM of GSA information systems and data.
1.3 Policy

CM is covered in Chapter 4, paragraph 2 of CIO 2100.1 as stated in the following paragraph.

1. Configuration management.

(1) A system configuration management plan must be developed, implemented, and maintained for every IT system managed by GSA.
(2) All information systems must be securely hardened and patched before being put into operation and while in operation.
(3) GSA information systems, including vendor owned/operated systems on behalf of GSA, must configure their systems in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate. Where a GSA benchmark exists, it must be used. GSA benchmarks may be exceeded but not lowered.
(4) Develop the configuration management plan IAW GSA-CIO-IT Security-01-05.

1.4 References

Federal Laws and Regulations:
• EO 13800, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”

Federal Standards and Guidance:
• FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems”
• NIST SP 800-37, Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems”
• NIST SP 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations”
• Cybersecurity Framework, “Framework for Improving Critical Infrastructure Cybersecurity”

GSA Directives, Policies, and Procedures:
• GSA Order CIO 2100.1, “GSA Information Technology (IT) Security Policy”
• GSA CIO Order 2108.1, “CIO Software License Management.”
• GSA Order CIO 2140.4, “Information Technology (IT) Solutions Life Cycle (SLC) Policy”
• CIO-IT Security-06-30, “Managing Enterprise Risk”
• GSA ISPP, “Information Security Program Plan”

2 Roles and Responsibilities

There are many roles associated with implementing an effective CM process for IT 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. Throughout this guide, specific processes and procedures for implementing CM with a security focus are described.

2.1 Chief Information Security Officer (CISO)

Responsibilities include the following:

- Implementing and overseeing GSA's IT Security Program by developing and publishing IT Security Procedural Guides that are consistent with CIO 2100.1;
- Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

2.2 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.
- Accepting the risk of operating GSA information systems under their purview where CM controls have not been fully implemented.
- Ensuring a plan of action and milestones (POA&M) item is established and managed to address CM controls that are not fully implemented.

2.3 Information System Security Manager (ISSM)

Responsibilities include the following:

- Coordinating with ISSOs to establish and manage processes and procedures supporting CM controls for all systems under their purview.
- Monitoring and supporting the resolution of POA&Ms to mitigate system vulnerabilities regarding CM controls for all systems under their purview.
- Ensures GSA IT security policies and procedures are followed.

2.4 Information System Security Officer (ISSO)

Responsibilities include the following:

- Ensuring necessary CM security controls are in place and operating as intended.
- Developing POA&Ms, when necessary, regarding CM controls for all systems under their purview.
- Assisting system owners in developing and maintaining CM Plans, as necessary.
- Assisting system owners, AOs, and the Configuration Control Board (CCB) in performing or coordinating the performance of security impact analyses of requested changes when necessary.
2.5 System Owners (e.g., System Program Managers/Project Managers)

Responsibilities include the following:

- Ensuring necessary CM controls are in place and operating as intended.
- Developing and implementing a configuration management plan for their respective systems.
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for their respective systems.
- Ensuring that for each information system, security is planned, documented, and integrated into the solutions life cycle (SLC) from the information system’s initiation phase to the system’s disposal phase.
- Participating as a leading member on the CCB.
- Assisting with the preparation of the CCB charter and selection of its members.

2.6 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.

3 Configuration Management Overview

CM manages the changes to hardware, software, and documentation of an information system or network throughout its lifecycle. CM 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 an information 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 and require updates to system documentation to reflect the changes and 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 authorized. GSA follows the guidance in NIST 800-37, Revision 1, Appendix F, Section F.6 when determining what qualifies as a significant change.

### 3.1 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 five phases as listed on the [GSA Project Management Life Cycle](https://www.gsa.gov/projectmanagementlifecycle) webpage. The five phases of the SLC and their relationship to the NIST RMF Steps are listed in Table 3-1. Details of each phase and SLC documentation templates are available on the [GSA IT Enterprise Program Management Office (ePMO) Templates](https://www.gsa.gov/epmo) webpage. 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 reduce risks during the operation and maintenance of information systems.

<table>
<thead>
<tr>
<th>SLC PHASE</th>
<th>RMF Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1 – Concept Approval</td>
<td></td>
</tr>
<tr>
<td>Identifies a business need requiring IT as part of the solution.</td>
<td>None.</td>
</tr>
<tr>
<td>Phase 2 – Initiation</td>
<td></td>
</tr>
<tr>
<td>Formally defines and authorizes a project.</td>
<td>Step 1 – Categorize Information System</td>
</tr>
<tr>
<td>Phase 3 – Planning</td>
<td></td>
</tr>
<tr>
<td>Clarifies the project’s objectives and plans all of the activities necessary to implement it.</td>
<td>Step 2 – Select Security Controls Step 3 – Implement Security Controls Step 4 – Assess Security Controls</td>
</tr>
<tr>
<td>Phase 4 – Execution</td>
<td></td>
</tr>
<tr>
<td>Deliverables are physically built and presented to the customer for acceptance.</td>
<td>Step 3 – Implement Security Controls Step 4 – Assess Security Controls Step 5 – Authorize Information System Step 6 – Monitor Security Controls</td>
</tr>
<tr>
<td>Phase 5 – Project Closeout</td>
<td></td>
</tr>
<tr>
<td>Consists of the processes to formally end the project and hand-off the operations to the appropriate team.</td>
<td>Step 4 – Assess Security Controls Step 5 – Authorize Information System Step 6 – Monitor Security Controls</td>
</tr>
</tbody>
</table>

Although the RMF steps in Table 3-1 are portrayed linearly with respect to the phases in the SLC, the actual implementation is iterative. For example, during Step 6 – Monitor Security Controls, 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 would require Steps 3-6 be completed for the additional controls.
4 Implementation Guidance for CM Controls

The GSA-defined parameter settings included in the control requirements are offset by brackets in the control text. As stated in Section 1.2, Scope, the requirements in this guide apply to GSA Federal employees and contractors who are involved in CM of GSA information systems and data. The GSA implementation guidance stated for each control applies to personnel and/or the systems operated on behalf of GSA. Any additional instructions/requirements for contractor systems will be included in the “Additional Contractor System Considerations” portion of each control section. If “None” is listed for “Additional Contractor System Considerations” it means there are no additional requirements, the system still needs to comply with the overall implementation guidance.

CM-1, Configuration Management Policy and Procedures, has been identified as a Common Control for all GSA/internally operated systems by GSA and as a Hybrid Control for contractor systems. The CM-2 to CM-11 controls, when included in a system’s control set, either are provided as a Common Control by a Major Information System, a system specific control by the system, or as a Hybrid Control with shared responsibilities for control implementation. GSA’s Information Security Program Plan (ISPP) describes the GSA enterprise-wide inheritable common and hybrid controls and outlines the responsible party for implementing each of them.

Note on Significant Changes: Systems that have a significant change as defined in NIST SP 800-37, Revision 1, Appendix F, Section F.6, will require reauthorization in accordance with GSA Order CIO 2100.1, and CIO-IT Security-06-30.

4.1 CM-1 Configuration Management Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to [Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers, Acquisitions/Contracting Officers, Custodians):

1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

b. Reviews and updates the current:

1. Configuration management policy [biennially]; and
2. Configuration management procedures [biennially].

GSA Implementation Guidance: Control CM-1 is applicable at all FIPS 199 levels.

Common Control Implementation:
Configuration Management (CM) policies and procedures is a common control provided by the OCISO Policy and Compliance Division (ISP). CM Policy is included in the current GSA Order CIO
2100.1, Chapter 4, Policy on Operational Controls. The policy states: "A system CM plan must be developed, implemented, and maintained for every IT system managed by GSA". GSA OCISO ISP has also defined agency-wide CM procedures in GSA IT Security Procedural Guide 01-05, "Configuration Management" (this guide). GSA’s security policy and procedural guides are disseminated via the IT Security webpage.

GSA Service/Staff Office (S/SO) organizations are encouraged but not required to have separate CM policies and procedures to supplement procedures in the GSA IT Security Policy and the CM guide. Supplemental procedures may be unique to the S/SO, system, data type (Financial, Privacy, etc.) or convey the organizations implementation of common and/or hybrid controls as defined in the most current NIST SP 800-37.

GSA Order CIO 2100.1 and GSA IT Security Procedural Guide 01-05 are reviewed and updated biennially.

**Additional Contractor System Considerations:**

Vendors/Contractors may defer to the GSA policy and guide or implement their own CM control policies and procedures which comply with GSA’s requirements with the approval of the AO.

### 4.2 CM-2 Baseline Configuration

**Control**: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

**Control Enhancements:**

1. **Baseline Configuration | Reviews and Updates.** The organization reviews and updates the baseline configuration of the information system:
   (a) [Annually];
   (b) When required due to [significant change as defined in NIST SP 800-37 Revision 1, Appendix F, Section F.6]; and
   (c) As an integral part of information system component installations and upgrades.
2. **Baseline Configuration | Automation Support for Accuracy / Currency.** The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.
3. **Baseline Configuration | Retention of Previous Configurations.** The organization retains [GSA S/CO or Contractor recommended previous versions of baseline configurations of the information system approved by the GSA AO] to support rollback.
4. **Baseline Configuration | Configure systems, Components, or Devices for High-Risk Areas.** The organization:
   (a) Issues [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) Applies [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] to the devices when the individuals return.

**GSA Implementation Guidance:** Control CM-2 is applicable at all FIPS 199 levels. Enhancements CM-2(1), (2), (3) and (7) are applicable at FIPS 199 Moderate and High levels. CM-2(2) is applicable at the FIPS 199 Moderate level per GSA CISO mandate.

Baseline configurations are documented, reviewed, and agreed-upon sets of specifications for information systems or configuration items within those systems (i.e., what is on the component). Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. 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 EARC Approved 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 information system is linked to the GSA mission.

For FIPS 199 Moderate and High levels the following guidance applies.

- For enhancement CM-2(1), 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.
- For enhancement CM-2(2), GSA leverages existing enterprise security and CDM tools including BigFix and Tenable to maintain, manage, and verify baseline configurations.
- For enhancement CM-2(3), GSA systems must maintain previous versions of baseline configurations to support rollback capabilities.
- For enhancement CM-2(7), GSA Order 2100.1 anyone travelling to an area deemed high risk will be issued specially configured loaner devices which will be wiped immediately upon return.

**Additional Contractor System Considerations:**
Contractor systems not utilizing GSA configuration standards must provide their system baseline configuration to GSA for review and approval by the AO. The organization-defined setting for CM-2(3), deferred for a system-specific recommendation by the GSA S/IO/Contractor, must be approved by the GSA AO before implementation.
4.3 CM-3 Configuration Change Control

Control: The organization:

a. Determines the types of changes to the information system that are configuration controlled;

b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

c. Documents configuration change decisions associated with the information system;

d. Implements approved configuration-controlled changes to the information system;

e. Retains records of configuration-controlled changes to the information system for [as long as deemed necessary by GSA S/SO or Contractor and approved by the GSA AO];

f. Audits and reviews activities associated with configuration-controlled changes to the information system; and

g. Coordinates and provides oversight for configuration change control activities through [a charted Configuration Change Board (CCB)] that convenes [on a monthly basis monitoring the following conditions]:

- Changes to the information system, including upgrades, modifications;
- Changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers);
- Emergency Changes; and
- Changes to remediate flaws.

Control Enhancements:

(1) Configuration Change Control | Automated Document / Notification / Prohibition of Changes. The organization employs automated mechanisms to:

(a) Document proposed changes to the information system;

(b) Notify [GSA S/SO or Contractor recommended approval authorities approved by the GSA AO] of proposed changes to the information system and request change approval;

(c) Highlight proposed changes to the information system that have not been approved or disapproved by [GSA S/SO or Contractor recommended time period approved by the GSA AO];

(d) Prohibit changes to the information system until designated approvals are received;

(e) Document all changes to the information system; and

(f) Notify [Administrators (Application, System, Network, etc.), Information System Security Officer, Information System Security Manager, System Owner (e.g., System Program Manager, System Project Manager)] when approved changes to the information system are completed.

(2) Configuration Change Control | Test / Validate / Document Changes. The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.
GSA Implementation Guidance: Control CM-3 and CM-3(2) are applicable at the FIPS 199 Moderate and High levels. Enhancement CM-3(1) is applicable at the FIPS 199 High level.

Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. This control focuses on defining the CM process, controlling the information 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 GSA InSite.

- Manage configuration changes to the information system through a chartered Configuration Control Board (CCB) that approves proposed changes to the system. The CCB should monitor the following:
  - Changes to the information 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 information system. Include emergency changes in the configuration change control process.
- Conduct a security impact analysis (per CM-4) 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 (Appendix A) is provided.
- 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 information 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 information system (perform the test on a test platform, not a production platform).

For enhancement CM-3(1), FIPS 199 High 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 system’s security and configuration management plans.

For enhancement CM-3(2), FIPS 199 Moderate and High systems are required to test, validate, and document changes before implementation in the operational environment.

**Additional Contractor System Considerations:**
None.

4.4 CM-4 Security Impact Analysis

**Control:** The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

**Control Enhancement:**

(1) Security Impact Analysis | Separate Test Environments. The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

**GSA Implementation Guidance:** Control CM-4 is applicable at all FIPS 199 levels. Enhancement CM-4(1) is applicable at the FIPS 199 High level.

The focus of this control is conducting security impact analyses prior to implementing any change (including patches, upgrades, and modifications) to the information system and checking the security features of the system after changes have been implemented. Below are some general guidelines:

- Employ measures for documenting and monitoring changes to the information system in the System Security Plan (SSP) or CM plan.
- Analyze changes to the information system to determine potential security impacts prior to change implementation and as part of the change approval process.
- Ensure security impact analyses are conducted by personnel with the proper information security responsibilities.
- Ensure individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications.
- Ensure that the Security Impact Analysis includes activities such as:
  - Reviewing information system documentation such as the SSP 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 security impact analysis in accordance with the impact level of the information system.
- Ensure information system security features are verified to confirm they are still functioning properly after the system is changed (including upgrades and modifications).

For enhancement CM-4(1) FIPS 199 High systems must analyze changes in a separate test environment before implementation in an operational environment.

**Additional Contractor System Considerations:**
None.

### 4.5 CM-5 Access Restrictions for Change

**Control:** The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

**Control Enhancements:**

1. **Access Restrictions for Change | Automated Access Enforcement / Auditing.** The information system enforces access restrictions and supports auditing of the enforcement actions.
2. **Access Restrictions for Change | Review System Changes.** The organization reviews information system changes *[at least weekly]* and *[when indications so warrant]* to determine whether unauthorized changes have occurred.
3. **Access Restrictions for Change | Signed Components.** The information system prevents the installation of *[GSA S/SO or Contractor recommended software and firmware components approved by the GSA AO]* without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

**GSA Implementation Guidance:** Control CM-5 is applicable at the FIPS 199 Moderate and High levels. Enhancement CM-5(1), (2), and (3) are applicable at the FIPS 199 High level.

The focus of this control is to restrict the ability to make changes to the information system. 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-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the information 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 information system;
- System upgrades; and
- System modifications.
For enhancements CM-5(1), (2), and (3) FIPS 199 High systems must implement automated and manual processes to restrict and audit changes, review changes, and prevent installation of unauthorized components.

**Additional Contractor System Considerations:**
None.

### 4.6 CM-6 Configuration Settings

**Control:** The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using [GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as deemed appropriate by the GSA AO (implemented checklists must be integrated with Security Content Automation Protocol (SCAP) content)] that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for [all components] based on [explicit operational requirements]; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

**Control Enhancements:**

1. **Configuration Settings | Automated Central Management / Application / Verification.** The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [operating systems].
2. **Configuration Settings | Respond to Unauthorized Changes.** The organization employs [configuration management/continuous monitoring/continuous diagnostics and mitigation tool agents (e.g., FireEyeHX, BigFix) installed and integrated into GSA's Enterprise Logging Platform for internal agency systems, for external vendor/contractor systems, similar tools/agents should be monitored using an ELP or ELP-like tool] to respond to unauthorized changes to [configuration settings as specified in CM-6a].

**GSA Implementation Guidance:** Control CM-6 is applicable at all FIPS 199 levels. Enhancement CM-6(1) is applicable at the FIPS 199 Moderate and High levels. CM-6(1) is applicable at the FIPS 199 Moderate level per GSA CISO mandate. Enhancement CM-6(2) is applicable at the FIPS 199 High level.

**Common Control Implementation:**
Configure 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 deemed appropriate by the AO. Configure the security settings to the
most restrictive mode consistent with operational requirements in all components of the information system.

Security settings that are not completely implemented because of operational requirements should be documented in the SSP. 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 CM Plan 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 resolution.

For enhancements CM-6(1) and (2), GSA uses automated tools such as FireEyeHX and BigFix that are installed and integrated into GSA's Enterprise Logging Platform to verify configuration settings and alert personnel to respond to unauthorized changes.

System Specific Expectations:
The System Owner is responsible for implementing the configuration settings as stated for this control and maintaining configuration control and managing changes using a configuration management process and plan. 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 system Information System Security Officer/Information System Security Manager (ISSO/ISSM).
- Deviations to CIS Level 2 settings can be reviewed and approved by the ISSO and ISSM with appropriate justification.
- Deviations to CIS Level 1 settings require AO approval.

Additional Contractor System Considerations:
Vendor/Contractor systems not utilizing GSA, NIST, or CIS IT Security Hardening standards must provide their technical security hardening guidelines to GSA for review and approval by the AO.

4.7 CM-7 Least Functionality

Control: The organization:

a. Configures the information system to provide only essential capabilities; and
b. Prohibits or restricts the use of the following functions, ports, protocols, 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 AO].

Control Enhancements:

1. Least Functionality | Periodic Review. The organization:
   (a) Reviews the information system [quarterly] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
(b) Disables [GSA S/SO or Contractor recommended functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure as approved by the GSA AO].

(2) Least Functionality | Prevent Program Execution. The information system prevents program execution in accordance with [CIO 2100.1 policies and GSA S/SO 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; approved by the GSA AO].

(4) Least Functionality | Unauthorized Software/ Blacklisting. The organization:
   (a) Identifies [GSA S/SO or Contractor recommended software programs not authorized to execute on the information system as approved by the GSA AO];
   (b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and
   (c) Reviews and updates the list of unauthorized software programs [annually].

(5) Least Functionality | Authorized Software/ Whitelisting. The organization:
   (a) Identifies [GSA S/SO or Contractor recommended software programs authorized to execute on the information system as approved by the GSA AO];
   (b) Employs an allow-all, deny-by-exception policy to prohibit the execution of authorized software programs on the information system; and
   (c) Reviews and updates the list of authorized software programs [annually].

GSA Implementation Guidance: Control CM-7 is applicable at all FIPS 199 levels. Enhancements CM-7(1), (2) and (4) are applicable at the FIPS 199 Moderate level. Enhancements CM-7(1), (2), and (5) are applicable at the FIPS 199 High level.

The focus of this control is to reduce the attack surface available to be exploited and to restrict the functions and capabilities available to those that are authorized. The information system and each of its components should provide only the minimum 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).

Prohibited or restricted functions, ports, protocols, and/or services should be specifically defined in the system’s SSP. Technical security configurations are documented in GSA, NIST, and Center for Internet Security guidelines, or industry best practice guidelines as deemed appropriate by the GSA AO.

For enhancements CM-7(1) and (2) FIPS 199 Moderate and High level systems must:

- Conduct a quarterly review of the functions, ports, protocols, and services provided and disable any the AO does not approve as necessary.
- Prevents 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 AO.
For enhancement CM-7(4) FIPS 199 Moderate level systems must use blacklisting and for enhancement CM-7(5) FIPS 199 High level systems must use whitelisting capabilities to deny unauthorized software and allow authorized software to execute on the system. GSA uses automated tools (e.g. Bit9, Tripwire) to support blacklisting and whitelisting of software.

**Additional Contractor System Considerations:**
None.

### 4.8 CM-8 Information System Component Inventory

**Control:** The organization:

a. Develops, documents, and maintains an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components within the authorization boundary of the information system;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
   4. Includes [GSA S/SO or Contractor recommended information deemed necessary to ensure property accountability as approved by the GSA 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. Reviews and updates the information system component inventory *(quarterly).*

**Control Enhancements:**

1. Information System Component Inventory | Updates During Installations / Removals. The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.
2. Information System Component Inventory | Automated Maintenance. The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.
3. Information System Component Inventory | Automated Unauthorized Component Detection. The organization:
   a. Employs automated mechanisms *[on a quarterly basis]* to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
   b. Takes the following actions when unauthorized components are detected: *[isolates the components and notifies Information System Security Manager, Information System Security Officer, System Owners (e.g., System Program Managers, System Project Managers), and Custodians].*
4. Information System Component Inventory | Accountability Information. The organization includes in the information system component inventory information, a
means for identifying by [name, position, and role], individuals responsible/accountable for administering those components.

(5) Information System Component Inventory | No Duplicate Accounting of Components. The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

(6) Information System Component Inventory | Assessed Configurations / Approved Deviations. The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

**GSA Implementation Guidance**: Control CM-8 is applicable at all FIPS 199 levels. Enhancements CM-8(1), (2), (3), (5) and (6) are applicable at the FIPS 199 Moderate and High levels. Enhancement CM-8(4) is also applicable at the FIPS 199 High Level. CM-8(2) and (6) are applicable at the FIPS 199 Moderate level per GSA CISO mandate, as is CM-8(6) at the FIPS 199 High level.

The focus of this control is maintaining control of the components in the information system. The first step is to identify all components of the information system within the authorization boundary and its relevant ownership information. Include any information determined to be necessary to achieve effective accountability. Determine the appropriate level of granularity for the 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
- Information system/component owner
- Machine name and network address (if a network device).

The information system component inventory is defined in Section 10 of the system’s SSP, System Environment. Information systems must maintain an up-to-date component inventory. 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 at least quarterly. As GSA implements its Continuous Diagnostics and Mitigation (CDM) tools they will be key in having up to date inventories.

For enhancements CM-8 (1), (2), (3), (5) and (6) systems at the FIPS 199 Moderate and High levels must:

- Update the inventory during installations, removals, and system updates (i.e., not just quarterly).
- Use the GSA automated tools identified in the main control implementation details to maintain the inventory.
- Use the same GSA automated tools or other automated tools to detect unauthorized components at least on a quarterly basis, 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 that components are not duplicated across system inventories.
- Includes the “as-is” state of components (i.e., assessed configurations and approved deviations) in the inventory.

For enhancement CM-8 (4) systems at the FIPS 199 High level must include in the inventory the name, position, and role of the administrator of the component.

**Additional Contractor System Considerations:**
None.

### 4.9 CM-9 Configuration Management Plan

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

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification.

**GSA Implementation Guidance:** Control CM-9 is applicable at all FIPS 199 levels. CM-9 is applicable at the FIPS 199 Low level per GSA CIO Order 2100.1.
A system CM plan must be developed, implemented, and maintained for every IT system managed by GSA. System owners must ensure the system’s CM Plan addresses the NIST SP 800-53 CM control requirements applicable to it based on its FIPS 199 level. The CM Plan must:

- Address roles and responsibilities for CM of the system.
- Identify the Configuration Items (CIs) to be placed under CM for the information system.
- Describe the CM processes and procedures used to manage the system’s baseline.
- Defines how change control is managed and communicated.
- Defines how configuration status accounting and auditing is maintained.
- Describes how CM is managed throughout a systems life cycle.

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

A CM Plan Template is available on GSA InSite.

**Additional Contractor System Considerations:**
None.

### 4.10 CM-10 Software Usage Restrictions

**Control:** The organization:

- Uses software and associated documentation in accordance with contract agreements and copyright laws;
- Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
- Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

**GSA Implementation Guidance:** Control CM-10 is applicable at all FIPS 199 levels.

GSA uses standard configurations for workstations and servers to establish the authorized/approved software for systems. GSA’s technical hardening guidelines and tools (e.g., Bit9, Tripwire) are used to prohibit users from installing unauthorized/copyright protected software. 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 tools (e.g., Tripwire, Bit9) to prohibit installation of such technologies.

**Additional Contractor System Considerations:**
None.
4.11 CM-11 User-Installed Software

**Control:** The organization:

a. Establishes \( \text{[policies as specified in CIO 2100.1]} \) governing the installation of software by users;

b. Enforces software installation policies through \( \text{[automated methods (i.e., configuration/compliance scans)]} \); and

c. Monitors policy compliance at \( \text{[least quarterly]} \).

**GSA Implementation Guidance:** Control CM-11 is applicable at all FIPS 199 levels.

Chapter 4, Policy on Operational Controls, Section 2.o, Software and digital media acceptable use, of CIO 2100.1 provides policy guidance regarding the installation of software by users. Effectively, GSA users may only install/use software that is approved and registered for GSA use and must be received from GSA approved sources.

GSA uses tools (e.g., Tripwire, Bit9) to prohibit users from installing software and GSA’s hardening guide settings and compliance/configuration checks performed by additional tools (e.g., BigFix, Tenable Security Center) are used to enforce GSA’s software installation policies and identify violations for remediation. GSA monitors data from these tools regularly and, at a minimum, determines the tools are collecting the appropriate data and systems are complying with software usage restrictions. As GSA’s CDM processes mature the toolsets and monitoring, and reporting capabilities will allow more frequent monitoring and enforcement.

**Additional Contractor System Considerations:**

None.

5 Summary

An effective CM plan, procedures, and processes supports maintaining the security of the system by considering security throughout a system’s life cycle. This guide is describes how security is included by establishing guidance on implementing the NIST SP 800-53 CM controls. The establishment of security as an integral part of CM establishes the requirements to configure systems securely at the start (i.e., configured securely in accordance with GSA technical guidelines), integrate securely by limiting functionality and installed software to the minimum required to meet operational needs, and maintain security by conducting security impact analyses as a part of change control.

All GSA systems must have a CM Plan as required by GSA CIO 2100.1 in order to allow information systems to maintain security as inevitable changes occur throughout the system’s life cycle.

GSA contractors and Federal employees should use this guide and the noted references prior to selecting implementing their CM plan and processes. Where there is a conflict between NIST
guidance and GSA guidance, contact the OCISO, ISP Division for guidance, at ispcompliance@gsa.gov.
Appendix A - Change Request Form

GSA uses automated tools (e.g., ServiceNow, JIRA), however for any systems which are unable to use an automated tool a Change Request Form has been developed and is available on the GSA InSite IT Security Forms page.
Appendix B – Configuration Management Plan Template

The Configuration Management Plan Template is located on GSA InSite.