

Department of the Interior
Security Control Standard
Configuration Management

April 2011

Version: 1.1



Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	Date:

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	December 17, 2010	Initial draft
Timothy Brown	0.2	December 27, 2010	Incorporated comments into text, removed non-mandated control enhancements
Timothy Brown	0.21	January 07, 2011	Added introductory paragraph
Timothy Brown	0.22	February 15, 2011	Checked/added moderate cloud to high
Chris Peterson	1.0	February 18, 2011	Final review of controls; removed margin notes. (several required controls still need defined values)
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY	3
TABLE OF CONTENTS	4
SECURITY CONTROL STANDARD: CONFIGURATION MANAGEMENT	5
CM-1 CONFIGURATION MANAGEMENT POLICIES AND PROCEDURES	5
CM-2 BASELINE CONFIGURATION	6
CM-3 CONFIGURATION CHANGE CONTROL	7
CM-4 SECURITY IMPACT ANALYSIS	8
CM-5 ACCESS RESTRICTIONS FOR CHANGE	9
CM-6 CONFIGURATION SETTINGS	10
CM-7 LEAST FUNCTIONALITY	11
CM-8 INFORMATION SYSTEM COMPONENT INVENTORY	12
CM-9 CONFIGURATION MANAGEMENT PLAN	13

SECURITY CONTROL STANDARD: CONFIGURATION MANAGEMENT

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Configuration Management (CM) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

CM-1 CONFIGURATION MANAGEMENT POLICIES AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

- a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the configuration management family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational

policies and procedures may make the need for additional specific policies and procedures unnecessary. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the configuration management policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW CM-1	MOD CM-1	HIGH CM-1
-----------	-----------------	-----------------	------------------

CM-2 BASELINE CONFIGURATION

Applicability: All Information Systems

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

Supplemental Guidance: This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with the organization's enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9.

Control Enhancements:

1. The organization reviews and updates the baseline configuration of the information system:
 - a. Annually;
 - b. When required due to a significant change; and
 - c. As an integral part of information system component installations and upgrades.
2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Enhancement Supplemental Guidance: Software inventory tools are examples of automated mechanisms that help organizations maintain consistent baseline configurations for information systems. Software inventory tools can be deployed for each operating system in use within the organization (e.g., on workstations, servers, network components, mobile devices) and used to track operating system version numbers, applications and types of software installed on the operating systems, and current patch levels. Software inventory tools can also scan information systems for

unauthorized software to validate organization defined lists of authorized and unauthorized software programs.

3. The organization retains older versions of baseline configurations as deemed necessary to support rollback.
4. The organization:
 - a. Develops and maintains [Assignment: organization-defined list of software programs not authorized to execute on the information system]; and
 - b. Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.
5. The organization:
 - a. Develops and maintains [Assignment: organization-defined list of software programs authorized to execute on the information system]; and
 - b. Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.
6. The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	LOW CM-2	MOD CM-2 (1) (3) (4) (5)	HIGH CM-2 (1) (2) (3) (5) (6)
-----------	-----------------	---------------------------------	--------------------------------------

CM-3 CONFIGURATION CHANGE CONTROL

Applicability: Moderate and High Impact Information Systems

Control: The organization:

- a. Determines the types of changes to the information system that are configuration controlled;
- b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;
- c. Documents approved configuration-controlled changes to the system;
- d. Retains and reviews records of configuration-controlled changes to the system;
- e. Audits activities associated with configuration-controlled changes to the system; and
- f. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection: (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

Supplemental Guidance: The organization determines the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology

products (e.g., operating systems, applications, firewalls, routers), emergency changes, and changes to remediate flaws. A typical organizational process for managing configuration changes to the information system includes, for example, a chartered Configuration Control Board that approves proposed changes to the system. Auditing of changes refers to changes in activity before and after a change is made to the information system and the auditing activities required to implement the change. Related controls: CM-4, CM-5, CM-6, SI-2.

Control Enhancements:

1. The organization employs automated mechanisms to:
 - a. Document proposed changes to the information system;
 - b. Notify designated approval authorities;
 - c. Highlight approvals that have not been received by **[Assignment: organization-defined time period]**;
 - d. Inhibit change until designated approvals are received; and
 - e. Document completed changes to the information system.

2. The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Enhancement Supplemental Guidance: The organization ensures that testing does not interfere with information system operations. The individual/group conducting the tests understands the organizational information security policies and procedures, the information system security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. An operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. In situations where the organization cannot conduct testing of an operational system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD CM-3 (2)	HIGH CM-3 (1) (2)
-----------	-------------------------	---------------------	--------------------------

CM-4 SECURITY IMPACT ANALYSIS

Applicability: All Information Systems

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

Supplemental Guidance: Security impact analyses are conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security

ramifications. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system. Related controls: CA-2, CA-7, CM-3, CM-9, SI-2.

Control Enhancements:

1. The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Enhancement Supplemental Guidance: Changes include information system upgrades and modifications.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P2	LOW CM-4	MOD CM-4	HIGH CM-4 (1)
-----------	-----------------	-----------------	----------------------

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Applicability: Moderate and High Impact Information Systems

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

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries. Examples of access restrictions include, for example, 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). Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes. Related controls: AC-3, AC-6, PE-3.

Control Enhancements:

1. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.
2. The organization conducts audits of information system changes [Assignment: organization defined frequency] and when indications so warrant to determine whether unauthorized changes have occurred.
3. The information system prevents the installation of [Assignment: organization-defined critical software programs] that are not signed with a certificate that is recognized and approved by the organization.
5. The organization:
 - a. Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and
 - b. Reviews and reevaluates information system developer/integrator privileges at least quarterly.

Enhancement Supplemental Guidance: Critical software programs and/or modules include, for example, patches, service packs, and where applicable, device drivers.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD CM-5 (1) (5)	HIGH CM-5 (1) (2) (3) (5)
-----------	-------------------------	-------------------------	----------------------------------

CM-6 CONFIGURATION SETTINGS

Applicability: All Information Systems

- a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using United States Government Configuration Baseline checklists that reflect the most restrictive mode consistent with operational requirements;
- b. Implements the configuration settings;
- c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
- d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information system are derived. A *security configuration checklist* (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by information technology developers and vendors, consortia, academia, industry, federal agencies (and other government organizations), and others in the public and private sectors. An example of a security

configuration checklist is the Federal Desktop Core Configuration (FDCC) which potentially affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: CM-2, CM-3, SI-4.

Control Enhancements:

1. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.
2. The organization employs automated mechanisms to respond to unauthorized changes to **[Assignment: organization-defined configuration settings]**.

Enhancement Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring mandatory/organization-defined configuration settings, or in the extreme case, halting affected information system processing.

3. The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

Enhancement Supplemental Guidance: Related controls: IR-4, IR-5.

References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: NVD.NIST.GOV; WWW.NSA.GOV.

Priority and Baseline Allocation:

P1	LOW CM-6	MOD CM-6 (1) (3)	HIGH CM-6 (1) (2) (3)
-----------	-----------------	-------------------------	------------------------------

CM-7 LEAST FUNCTIONALITY

Applicability: All Information Systems

Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services:

- All Unencrypted Network Transactions used for authentication or for any sensitive agency information
- Telnet
- FTP (Unless Approved by OCIO).

Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations

limit component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by organizational information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., Universal Serial Bus [USB], File Transfer Protocol [FTP], Internet Protocol Version 6 [IPv6], Hyper Text Transfer Protocol [HTTP]) on information system components to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related control: RA-5.

Control Enhancements:

1. The organization reviews the information system at least quarterly to identify and eliminate unnecessary functions, ports, protocols, and/or services.
2. The organization employs automated mechanisms to prevent program execution in accordance with *[Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage]*.

Enhancement Supplemental Guidance: Related control: CM-2.

References: None.

Priority and Baseline Allocation:

P1	LOW CM-7	MOD CM-7 (1)	HIGH CM-7 (1) (2)
-----------	-----------------	---------------------	--------------------------

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Applicability: All Information Systems

Control: The organization develops, documents, and maintains an inventory of information system components that:

- a. Accurately reflects the current information system;
- b. Is consistent with the authorization boundary of the information system;
- c. Is at the level of granularity deemed necessary for tracking and reporting;
- d. Includes manufacturer, model number, serial number, software license information, system/component owner; and
- e. Is available for review and audit by designated organizational officials.

Supplemental Guidance: Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, 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. Related controls: CM-2, CM-6.

Control Enhancements:

1. The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.
2. The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Enhancement Supplemental Guidance: Organizations maintain the information system inventory to the extent feasible. Virtual machines, for example, can be difficult to monitor because they are not visible to the network when not in use. In such cases, the intent of this control enhancement is to maintain as up-to-date, complete, and accurate an inventory as is reasonable.

3. The organization:
 - a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the addition of unauthorized components/devices into the information system; and
 - b. Disables network access by such components/devices or notifies designated organizational officials.

Enhancement Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections in AC-17 and for unauthorized mobile devices in AC-19. The monitoring for unauthorized components/devices on information system networks may be accomplished on an ongoing basis or by the periodic scanning of organizational networks for that purpose. Automated mechanisms can be implemented within the information system and/or in another separate information system or device. Related controls: AC-17, AC-19.

4. The organization includes in property accountability information for information system components, a means for identifying by **[Selection (one or more): name; position; role]** individuals responsible for administering those components.
5. The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	LOW CM-8	MOD CM-8 (1) (3) (5)	HIGH CM-8 (1) (2) (3) (4) (5)
-----------	-----------------	------------------------------------	--------------------------------------

CM-9 CONFIGURATION MANAGEMENT PLAN

Applicability: Moderate and High Impact Information Systems

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. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and
- c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

Supplemental Guidance: Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The configuration management plan satisfies the requirements in the organization's configuration management policy while being tailored to the individual information system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. The plan describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated. The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system, and security personnel that would conduct an impact analysis prior to the implementation of any changes to the system. Related control: SA-10.

Control Enhancements: None mandated.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD CM-9	HIGH CM-9
-----------	-------------------------	-----------------	------------------