EPA INFORMATION PROCEDURES

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.:	CIO-2150.3-P-05.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

INFORMATION SECURITY –

INTERIM CONFIGURATION MANAGEMENT PROCEDURES

V2.1

JULY 17, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Configuration Management control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and*

2. SCOPE AND APPLICABILITY

These procedures cover all EPA information and information systems to include information and information systems used, managed, or operated by a contractor, another agency, or other organization on behalf of the agency.

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

3. AUDIENCE

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that all offices within the Agency meet the minimum security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the configuration management family of controls found in NIST SP 800-53, Revision 3.

Configuration management is the process of establishing and maintaining the technical integrity of an information system throughout its life cycle by systematically identifying,

controlling, and accounting for all changes made to the information system. A configuration management process for each General Support System (GSS) and Major Application (MA) will effectively manage and track system changes. A Configuration Management Plan (CMP) is an essential document that provides a structured method of documenting the configuration management process for a GSS or MA.

Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This allows agencies to improve information system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of government information.

In March 2007, the Office of Management and Budget (OMB) announced the "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems" in memorandum M-07-11. The memorandum directed agencies with Windows XPTM deployed and/or planning to upgrade to the Vista™ operating system to adopt the Federal Desktop Core Configuration (FDCC) security configurations developed by NIST, the Department of Defense (DoD), and the Department of Homeland Security (DHS).

OMB, in M-08-21 dated July 2008, required agencies to:

- Document in the annual FISMA report the extent to which information system configuration requirements have been implemented.
- Use published configurations or justify why it is not done.

In addition, agencies' Chief Information Officers (CIOs) were required to develop plans for Microsoft Windows XP and Vista to include:

- Testing configurations in a non-production environment to identify adverse effects on information system functionality.
- Implementing and automating enforcement for using these configurations.
- Restricting administration of these configurations to only authorized professionals.
- Ensuring new acquisitions include these configurations and require information technology providers to certify their products operate effectively using these configurations.
- Applying Microsoft patches available from DHS when addressing new Windows XP or Vista vulnerabilities.
- Providing NIST with documentation of any deviations from these configurations and rationale for doing so.
- Ensuring these configurations are incorporated into Agency capital planning and investment control processes.

OMB memorandum M-08-22, issued August 2008, required agencies to use Security Content Automation Protocol (SCAP) tools that had been validated by NIST, to scan for FDCC configurations and configuration deviations. Federal CIOs were also instructed to ensure that government application providers self-assert that currently supported versions of applications:

- Operate correctly on federal Windows XP and Windows Vista computer systems configured with FDCC.
- Do not change FDCC settings

Through time it is expected these FDCC requirements will be applied to additional platforms.

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III*, Federal Information Security Management Act (FISMA)* as amended
- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 USC 3501-3519)
- Privacy Act of 1974 (5 USC § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C— *Employees Responsible for the Management or Use of Federal Computer Systems*, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
- Office of Management and Budget (OMB) Memorandum M-06-16, "*Protection of Sensitive Agency Information",* June 2006
- OMB Memorandum M-07-11, "*Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*", March 2007
- OMB Memorandum M-07-18, "*Ensuring New Acquisitions Include Common Security Configurations"*, June 2007
- OMB Memorandum M-08-21, "*FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*", July 2008
- OMB Memorandum M-08-22, "*Guidance on the Federal Desktop Core Configuration (FDCC)",* August 2008
- OMB Memorandum for Chief Information Officers, "*Managing Security Risk By Using Common Security Configurations*", March 2007
- OMB Circular A-130, "*Management of Federal Information Resources*", Appendix III, "*Security of Federal Information Resources*", November 2000
- Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy

6. PROCEDURES

CM- 2 – Baseline Configuration

Note: This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects

of the system.

a. A current baseline configuration must be developed, documented, and maintained under configuration control for the information system.
b. The baseline configuration must include documented, up-to-date specifications to which the information system is built and configured.
c. The baseline configuration must document and provide information about the components of an information system including:
    i. Standard operating system/installed applications with current version numbers
    ii. Standard software load for workstations, servers, network components, and mobile devices and laptops
    iii. Up-to-date patch level information
    iv. Network topology
    v. Logical placement of the component within the system and enterprise architecture
    vi. Technology platform

Note: Individual units or elements of the component's makeup are known as Configuration Items (CIs). Refer to Section 9.

d. New baselines must be created as the information system changes over time as this includes maintaining the baseline configuration.
e. The baseline configuration of the information system must be consistent with EPA's enterprise architecture.

For moderate information systems

f. The EPA-defined list of software programs authorized to execute on the information system is currently developed and maintained at http://intranet.epa.gov/otop/itarchitecture/StandardsProfile.pdf
g. An allow-all, deny-by-exception authorization policy must be employed to identify software allowed to execute on the information system.

For moderate and high information systems

h. The baseline configuration of the information system must be reviewed and updated:
    i. Annually
    ii. When required due to changes in installed software and/or hardware
    iii. As an integral part of information system component installations and upgrades
    iv. When an increase in interconnection with other systems outside the authorization boundary or significant changes in the security requirements for the system.
i. Older versions of baseline configurations must be retained as deemed necessary to support rollback.

For high information systems

j. Automated mechanisms must be employed in order to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Note: 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.

k. The EPA-defined list of software programs authorized to execute on the information system is currently developed and maintained at http://intranet.epa.gov/otop/itarchitecture/StandardsProfile.pdf

l. A deny-all, permit-by-exception authorization policy must be employed to identify software allowed to execute on the information system.

m. A baseline configuration that is managed separately from the operational baseline configuration must be maintained for development and test environments.

CM-3 – Configuration Change Control

For moderate and high information systems

a. The types of changes to the information system that are to be configuration-controlled must be determined.

b. All changes to the information system that are determined to be configuration-controlled must be approved and documented.

   i. A CMP, also known as a Security Configuration Guide, must be developed to address all of the procedures in this chapter.

c. The approvals to implement a configuration-controlled change to the information system must include explicit consideration for the security impact analysis.

d. Records of configuration-controlled changes to the system must be retained and reviewed.

e. Oversight for configuration change control activities must be provided and coordinated through EPA's Change Advisory Board (CAB) that convenes at least once per month.

   i. Network infrastructure changes of identified CIs must be handled through EPA's Telecommunications Service Request (TSR) process.

Note: 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.

f. The configuration change control process for the information system must include a systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications.

g. Configuration change control must include changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers).
    i. Emergency changes, including changes resulting from the remediation of flaws, must be included in the configuration change control process.

h. Activities associated with configuration-controlled changes to the information system must be audited.

Note: 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.

i. Changes to the information system must be tested, validated, and documented before implementing the changes on the operational system.
    i. Testing must not interfere with information system operations.
    ii. The individual/group conducting the tests must understand EPA's information security policies and procedures, the information system security procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process.

Note: 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.

For high information systems

j. Automated mechanisms must be employed in order to:
    i. Document proposed changes to the information system.
    ii. Notify designated approval authorities.
    iii. Highlight approvals that have not been received within two (2) weeks/ten (10) business days.
    iv. Inhibit change until designated approvals are received.
    v. Document completed changes to the information system.

CM-4 – Security Impact Analysis

a. Prior to change implementation, changes to the information system must be analyzed to determine potential security impacts.

b. Security impact analyses must be 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.
    i. Individuals conducting security impact analyses must have the appropriate skills and technical expertise to analyze the changes to information system

and the associated security ramifications.

ii. The security impact analysis must be provided to the Information System Security Officer (ISSO) upon request to ensure that the ISSO is aware of any changes to the security controls which may impact the security posture of the information system.

c. The security impact analysis must include, but is not limited to:

i. Reviewing information system documentation to understand how specific security controls are implemented within the system and how changes might affect the controls.

ii. Assessing risk to understand the impact of the changes and to determine if additional security controls are required.

d. The security impact analysis must be scaled in accordance with the security categorization of the information system.

e. The baseline configuration and system components inventory, as defined in CM-2 and CM-8, must be changed only through an approved change control process.

For high information systems

f. New software looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice must be analyzed in a separate test environment before installation in an operational environment.

CM-5 – Access Restrictions for Change

For moderate and high information systems

Note: 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.

a. The System Owner (SO) shall define, document, approve, and enforce physical and logical access restrictions associated with changes (e.g., upgrades, modifications) to the information system.

i. Individuals authorized to perform configuration changes must be documented in the CMP.

ii. Logical and physical access control lists that authorize qualified individuals to make changes to an information system or component must be created and maintained.

iii. Only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes,

including upgrades, and modifications.

b. Access records must be maintained to ensure 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.
    i. All information system changes associated with access privileges for such changes must be reviewed.
    ii. The SO shall review and verify access lists quarterly and shall document any variances that are found.

Note: 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.

For high information systems

c. Automated mechanisms must be employed to enforce access restrictions and support auditing of the enforcement actions.
d. Audits of information system changes must be conducted semi-annually and when indications so warrant to determine whether unauthorized changes have occurred.
e. The information system must prevent the installation of defined critical software programs that is not signed with a certificate that is recognized and approved by EPA.

CM-6 – Configuration Settings

a. A standard set of mandatory configuration settings must be established and documented for information technology products employed within the information system.
    i. Standard Configuration Documents (SCDs) must detail the configuration settings.

Note: For definitions and explanations of configuration settings, security-related parameters, and security configuration checklist, refer to Section 9.

b. The selected configuration settings, whether agency standards or designed specifically for the information system, must reflect the most restrictive mode consistent with operational requirements and must be derived from the following sources, listed in order of precedence:
    i. Federally mandated and NIST-approved configuration standards and checklists:
        - NIST recommended configurations and checklists found at http://checklists.nist.gov/
        - Defense Information Systems Agency (DISA) security checklists and Standard Technical Implementation Guides (STIGs) found at http://iase.disa.mil/stigs/stig/index.html and http://iase.disa.mil/stigs/checklist/index.html
        - National Security Agency (NSA) configuration guides found at http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml

- Others as listed by NIST

ii. Voluntary consensus security configuration standards and benchmarks from a recognized independent body including, but not limited to:

- Computer Internet Security (CIS) found at http://www.cisecurity.org
- SANS Institute benchmarks and checklists found at http://www.sans.org/score/

Note: 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.

Note: For an explanation of consensus standards, refer to Section 9.

iii. Security configuration standards from a commercial product vendor for the vendor's specific commercial product.

- The configuration standards may be vendor consensus or vendor recommended.

iv. Agency recommended standard configurations.

v. Industry best practices.

Note: For a list of some acceptable standards, refer to Appendices B and C.

c. The SO may choose to employ configurations that exceed standards set forth in this document.

d. The source of the configuration standard employed must be documented in the CMP and System Security Plan (SSP).

e. Configuration settings must be implemented and exceptions from the mandatory configuration settings must be identified, documented, and approved for individual components within the information system based on explicit operational requirements.

f. Changes to the configuration settings must be monitored and controlled in accordance with EPA policies and procedures.

g. OMB FISMA reporting instructions, which are published annually (e.g., OMB M-07-19, M-08-21), must be used as guidelines on configuration requirements for federal information systems.

h. NIST SP 800-70, Revision 1 must be used for guidance on producing and using configuration settings for information technology products employed in information systems.

For moderate and high information systems

i. Detection of unauthorized, security-relevant configuration changes must be incorporated into the incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

For high information systems

j. Automated mechanisms must be employed to centrally manage, apply, and verify configuration settings

k. Automated mechanisms must be employed to respond to unauthorized changes to

defined configuration settings.

Note: 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.

CM-7 – Least Functionality

a. The information system must be configured to provide only essential capabilities.

b. The use of the following functions, ports, protocols, and/or services, at a minimum, must be specifically prohibited or restricted:

i. Domain Name System be (DNS)
- Port 53 / Transmission Control Protocol (TCP), User Datagram Protocol (UDP)

ii. File Transfer Protocol (FTP)
- Ports 20, 21 / TCP

iii. Hypertext Transfer Protocol (HTTP)
- Port 80 / TCP

iv. Internet Message Access Protocol (IMAP)
- Port 143 / TCP, UDP

v. Internet Relay Chat (IRC)
- Port 194 / UDP

vi. Network Basic Input Output System (NetBIOS)
- Port 137 / TCP, UDP

vii. Post Office Protocol 3 (POP3)
- Port 110 / TCP

viii. Session Initiation Protocol (SIP)
- Port 5060 / TCP, UDP

ix. Simple Mail Transfer Protocol (SMTP)
- Port 25 / TCP

x. Simple Network Management Protocol (SNMP)
- Port 161 / TCP, UDP

xi. Structured Query Language (SQL)
- Port 118 / TCP, UDP
- Port 156 / TCP, UDP

xii. Telnet
- Port 23 / TCP

Note: Some the functions and services, provided by default, may not be necessary to support essential organizational operations.

c. A list of the ports that are required to be left open must be maintained.

i. A statement of business necessity must be provided for each required port.

d. Where feasible, component functionality must be limited to a single function per device (e.g., email server or web server, not both).
    i. While it is sometimes cost effective to provide multiple services from a single component of an information system, doing so increases risk over limiting the services provided by any one component.
    ii. Use of multiple services from a single component must be specifically addressed in risk assessments.
        - Risks associated with using multiple services must be identified to the Authorizing Official (AO).
        - The risks associated with using multiple services must be accepted by the AO.

e. Functions and services provided by organizational information systems, or individual components of information systems, must be carefully reviewed in order to determine which functions and services are candidates for elimination.
    i. Examples of such functions and services are:
        - Voice over Internet Protocol (VoIP)
        - Instant Messaging
        - Auto-execute
        - File sharing

f. Unused and unnecessary physical and logical ports and protocols (e.g., Universal Serial Bus (USB), FTP, Internet Protocol Version 6 (IPv6), HTTP) on information system components must be considered for disabling to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling.

Note: Organizations can use 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.

For moderate and high information systems

g. The information system must be reviewed annually and unnecessary functions, ports, protocols, and/or services must be eliminated.

For high information systems

h. Automated mechanisms must be employed to prevent program execution in accordance with: list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage.

CM-8 – Information System Component Inventory

a. An inventory of information system components or CIs that accurately reflects the current information system must be developed, documented, and maintained.

Note: Configuration planning management responsibilities for various types of CIs can

be found in Appendix D.

b. The level of granularity deemed necessary for the information system components must be determined.
    i. As applicable, the owning organization assigns the owning information system's identification number to each item in the inventory.
        - This identification number may be in addition to the EPA property number, if applicable.

c. The inventory of information system components must be updated as an integral part of the component installations, removals, and information system updates.

d. The inventory of information system components must include any information determined to be necessary by the organization to achieve effective property accountability including, but not limited to:
    i. Manufacturer
    ii. Type
    iii. Model
    iv. Serial number
    v. Physical location
    vi. Software license information
    vii. Information system/component owner
    viii. Associated component configuration standard
    ix. Software/firmware version information
    x. Networked component/device machine name or network address

e. The component inventory must be consistent with the authorization boundary of the information system.

f. The inventory of information system components must be available for review and audit by designated EPA officials.

For moderate and high information systems

g. All components within the authorization boundary of the information system must be verified either as part of the system or recognized by another system as a component within that system

For high information systems

h. Automated mechanisms must be employed to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

i. Automated mechanisms must be employed daily to detect the addition of unauthorized components/devices into the information system.

Note: 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.

j. The detection of unauthorized components/devices must result in either:
    i. Disabling network access; or
    ii. Notifying designated EPA officials.

k. Individuals responsible for administering information system components must be identified by name; position; and role; and included in property accountability information for those components.

CM-9 – Configuration Management Plan

For moderate and high information systems

a. A CMP for the information system must be developed, documented, and implemented.
    i. The CMP must satisfy the requirements in EPA's configuration management policy while being tailored to the individual information system.

b. The CMP must address roles, responsibilities, and configuration management processes and procedures.

c. The CMP must define detailed processes and procedures for how configuration management is used to support development life cycle activities at the information system level.
    i. The CMP must define the CIs for the information system and when the CIs are placed under configuration management in the system development life cycle.
        - The CMP must establish the means for identifying CIs throughout the system development life cycle and a process for managing the configuration of the CIs.

d. The CMP must describe:
    i. How to move a change through the change management process.
    ii. How configuration settings and configuration baselines are updated.
    iii. How the information system component inventory is maintained.
    iv. How development, test, and operational environments are controlled.
    v. How documents are developed, released, and updated.

e. The configuration management approval process must include:
    i. Designation of key management stakeholders who are responsible for reviewing and approving proposed changes to the information system.
    ii. Designation of security personnel that would conduct an impact analysis prior to the implementation of any changes to the system.

7. RELATED DOCUMENTS

- NIST SP 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009

- NIST SP 800-70 Revision 1, *National Checklists Program for IT Products: Guidelines for Checklists Users and Developers*, September 2009

8. ROLES AND RESPONSIBILITIES

Director of Office of Technology Operations and Planning (OTOP), Office of the Environmental Information (OEI)

a. The Director of OTOP/OEI is the authority for configuration management for IT standard resources and has the following responsibilities, which may be delegated to subordinate management with respect to configuration management:
   i. In consultation with the SAISO, develop standard configuration requirements and support the SAISO in verifying that the requirements are implemented appropriately.
   ii. Establish Configuration Control Review Boards (CCRB) and may be involved in the selection of the CCRB members.
   iii. Review the EPA baseline configuration documentation on an annual basis.
   iv. Manage configuration changes to the IT standard resources and OTOP managed information systems using an EPA or organization approved process, as appropriate.
   v. Monitor changes to the IT standard resources and OTOP managed information systems conducting security impact analyses to determine the effects of the changes.
   vi. Analyze changes to the IT standard resources and OTOP managed information system for potential security impacts.
   vii. Ensure that the baseline enterprise wide configuration and information system components inventory are only changed using an approved change control process.
   viii. Approve and enforce physical and logical access restrictions associated with changes to the OTOP managed information system.
   ix. Generate and retain records reflecting any changes associated with the individual's access privileges.
   x. Review configurations on an annual basis to identify and eliminate unnecessary functions, ports, protocols, and/or services.
   xi. Coordinate changes with the enterprise architecture planning and contingency planning functions.

Senior Agency Information Security Officer (SAISO)

b. The SAISO has the following responsibilities with respect to configuration management:
   i. Consult with OTOP management and staff concerning configuration management.
   ii. Provide oversight to the enterprise on the configuration management

process.

Authorizing Official (AO)

c. The AO has the following responsibilities with respect to configuration management:
    i. Determine whether to accept risks associated with providing multiple services from a single component of an information system.

System Owner (SO)

d. The SO is the authority for configuration management for the GSS or MA, as appropriate and has the following responsibilities with respect to configuration management:
    i. Develop functional requirements and verify that the requirements are implemented appropriately.
        1. This individual may also play a role in establishing the CCRB and may be involved in the selection of the CCRB members.
    ii. Review the baseline configuration documentation annually.
    iii. Manage configuration changes to the information system using an EPA or organization approved process as appropriate.
    iv. Monitor changes to the information system by conducting security impact analyses to determine the effects of the changes.
        1. Analyze changes to the information system for potential security impacts prior to change implementation and as part of the change approval process.
    v. Ensure that the baseline configuration and information system components inventory are only changed using an approved change control process.
    vi. Approve access privileges associated with changes to the information system.
    vii. Document individuals authorized to perform configuration changes in the CMP.
    viii. Enforce physical and logical access restrictions associated with changes to the information system.
    ix. Generate and retain records reflecting all changes associated with the individual's access privileges.
    x. Review and verify access lists quarterly and document any variances that are found.
    xi. Review the information system annually to identify and eliminate unnecessary functions, ports, protocols, and/or services.
    xii. Coordinate changes with the architecture planning and contingency planning functions.
    xiii. Develop, document, and implement a CMP that is tailored for the individual information system.
    xiv. Ensure that deviations from federal, NIST, or EPA-approved configuration

checklists and standards, if required by management in support of mission needs/objectives, are approved, documented in the CMP, and reported.

xv. Ensure that the source of the baseline configuration standard is documented in the CMP.

xvi. Address uses of multiple services in risk assessments and identify any risks associated with using multiple services to the AO.

Information System Security Officer (ISSO)

e. The ISSO has the following responsibilities with respect to configuration management:

i. Maintain a list of ports that are required to be left open, along with a statement of business necessity.

ii. Review security impact analyses.

iii. Ensure that configuration management activities delegated by the SO are carried out.

iv. Implement configuration requirements in the information system.

Users / Individuals

f. Users/individuals have the following responsibilities with respect to configuration management:

i. Report any weaknesses that are identified in current versions of the hardware, software, and components.

9. DEFINITIONS

- Baseline Configuration – a significant state of an information system's configuration history. The state may encompass hardware, software, firmware, documentation or a combination of IT assets. Baselines are usually formally approved states. Baselines may be standards for commercially available IT assets.
- Configuration Control – process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
- Configuration Item (CI) – a component of system inventory that is part of a baseline configuration and is under configuration management control, e.g., hardware, software, firmware, documentation. A CI may also be a combination of IT assets. CIs include EPA standard technologies (current, proposed or legacy), and technologies and architectures within EPA's Enterprise Architecture. A CI may depend on and have relationships with other IT assets and thus have hierarchical or relationship-based attributes assigned by the configuration manager. A CI has versions, based on changes implemented.
- Configuration Settings – the configurable security-related parameters of information technology products that are part of the information system.
- Consensus Standard – a standard developed or adopted by a standards body that through formal processes characterized by openness, balance of interest, due

process, an appeals process, and consensus. Consensus is marked by processes to resolve objections through fair consideration of all comments.

- Security Configuration Checklist – a series of instructions or procedures for configuring an information system component to meet operational requirements and is sometimes referred to as a lockdown guide, hardening guide, security guide, STIG, or benchmark.
- Security-Related Parameters – 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.
- Signature (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation. Can be accomplished manually (sometimes referred to as a "wet signature") or electronically.
- Written – or "in writing" means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- substantive business case need(s)
- demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

The SAISO and Director, OTOP shall coordinate to maintain central repository of all waivers.

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

Related policy and procedures are available on OEI's Policy Resources website.

http://intranet.epa.gov/oei/imitpolicy/policies.htm

Related standards and guidelines are available on OEI's website.

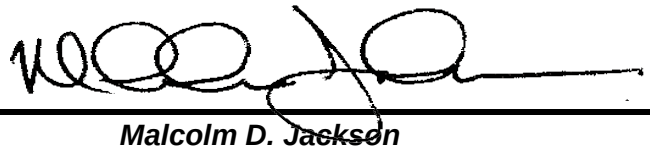
12. MATERIAL SUPERSEDED

EPA Information Security Manual, Directive 2195A1, 1999 Edition , Chapter 11, Section 11.2.3

13. ADDITIONAL INFORMATION

NA

EPA Classification No.:	CIO-2150.3-P-05.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015



Malcolm D. Jackson
Assistant Administrator and Chief Information Officer
Office of Environmental Information

APPENDIX A: ACRONYMS

AO	Authorizing Official
CCRB	Configuration Control Review Board
CI	Configuration Item
CIO	Chief Information Officer
CMP	Configuration Management Plan
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
EPA	Environmental Protection Agency
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
GSS	General Support System
HTTP	Hypertext Transfer Protocol
IPv6	Internet Protocol Version 6
ISSO	Information System Security Officer
IT	Information Technology
MA	Major Application
NetBIOS	Network Basic Input Output System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PC	Personal Computer
POP3	Post Office Protocol 3
OEI	Office of the Environmental Information
OMB	Office of Management and Budget
OTOP	Office of Technology Operations and Planning
SAISO	Senior Agency Information Security Officer
SCAP	Security Content Automation Protocol
SCD	Standard Configuration Document
SP	Special Publication
SQL	Structured Query Language
STIG	Standard Technical Implementation Guide
TCP	Transmission Control Protocol
TSR	Telecommunications Service Request
UDP	User Datagram Protocol
USB	Universal Serial Bus
USC	United States Code

APPENDIX B: APPROVED SECURITY CONFIGURATION STANDARDS FOR OPERATING SYSTEMS

Operating System	Operating System Configuration Standard	Location of Standard
AIX 5.2	AIX 5l Security Guide	http://publib16.boulder.ibm.com/pseries/en_US/aixbman/security/securitytfrm.htm
Cisco Router IOS	Improving Security On Cisco Routers, Cisco Systems	http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
Linux	Linux Security Resources	http://www.linuxsecurity.com/docs/
	Red Hat Enterprise Linux Security Guide	https://www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/security-guide/
	Debian Security Configuration Manual	http://www.debian.org/doc/user-manuals#securing
Solaris	NSA Guide To Secure Configuration Of Solaris	http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml
	U.S. Trusted Computer Systems Evaluation Criteria C2	http://docs.hp.com/en/B2355-90121/ch01s05.html
	Sun Solaris Security Toolkit	http://www.sun.com/software/security/jass/
	Sun Blueprints Online - Solaris Operating Environment Security	http://www.sun.com/blueprints/
Windows 2000	SANS Institute Top 20	http://www.sans.org/top20/
Windows 2000 Professional	NIST SP 800-43, *Systems Administration Guidance For Windows 2000 Professional*	http://csrc.nist.gov/publications/nistpubs/
	SANS Institute Top 20	http://www.sans.org/top20/

Operating System	Operating System Configuration Standard	Location of Standard
Windows 2000 Server	Microsoft Security Checklists	http://www.microsoft.com/technet/security/checklists/default.mspx
	DISA Checklist	http://iase.disa.mil/stigs/checklist/index.html
	U.S. Trusted Computer Systems Evaluation Criteria C2	http://docs.hp.com/en/B2355-90121/ch01s05.html
Windows 2003 Server	Microsoft Windows 2003 Security Guide	http://www.microsoft.com/downloads/details.aspx?familyid=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en http://www.microsoft.com/technet/security/topics/serversecurity/tcg/tcgch00.mspx
	Microsoft Security Checklists	http://www.microsoft.com/technet/security/checklists/default.mspx
	DISA Checklist	http://iase.disa.mil/stigs/checklist/index.html
Windows NT	SANS Institute Top 20	http://www.sans.org/top20/
Windows XP Professional	NIST SP 800-68, Revision 1, *Guidance For Securing Microsoft Windows XP Systems For IT Professionals*	http://csrc.nist.gov/publications/nistpubs/

APPENDIX C: APPROVED SECURITY CONFIGURATION STANDARDS FOR APPLICATIONS

Application	Application Configuration Standard	Location of Standard
Apache Jakarta Tomcat	Tomcat Server Configuration Reference	http://jakarta.apache.org/tomcat/tomcat-5.5-doc/config/index.html
Apache	NIST SP 800-44, Version 2, *Guidelines On Securing Public Web Servers*	http://csrc.nist.gov/publications/nistpubs/
Citrix	Citrix Security Bulletins And Guidelines	http://support.citrix.com/securitybulletins/
	DISA Checklist	http://iase.disa.mil/stigs/checklist/index.html
Informix	DISA Checklist	http://iase.disa.mil/stigs/checklist/index.html
	Informix Security And Encryption Guide	Version 10: http://publib.boulder.ibm.com/infocenter/idshelp/v10/index.jsp?topic=/com.ibm.jdbc_pg.doc/jdbc71.htm Version 11.5: http://publib.boulder.ibm.com/infocenter/idshelp/v115/index.jsp
Microsoft IIS	DISA Checklist	http://iase.disa.mil/stigs/checklist/index.html
	NIST SP 800-44, Version 2, *Guidelines On Securing Public Web Servers*	http://csrc.nist.gov/publications/nistpubs/
Microsoft Exchange	Microsoft Checklist - Securing Microsoft Exchange Communications	http://www.microsoft.com/technet/security/prodtech/exchangeserver/secmod47.mspx
	NIST SP 800-45, Version 2,*Guidelines On Electronic Mail Security*	http://csrc.nist.gov/publications/nistpubs/
Microsoft SQL	Microsoft Checklist - Securing Microsoft SQL Server	http://www.microsoft.com/technet/security/prodtech/sqlserver.mspx

Application	Application Configuration Standard	Location of Standard
	DISA Checklist	http://iase.disa.mil/stigs/checklist/index.html
Oracle	Oracle Paper, "A Security Checklist For Oracle11g." Oracle White Paper	http://www.oracle.com/technology/deploy/security/index.html
	Oracle Paper, "Hack Proofing Oracle."	http://www.oracle.com/technology/deploy/security/index.html
	Internet Security Systems, "Securing Database Servers"	www.iss.net
	"An Overview Of Oracle Database Security Features."	http://www.giac.org/certified_professionals/practicals/gsec/0740.php
WebLogic	WebLogic Security Guide	http://e-docs.bea.com/wls/docs81/security.html
WebSphere	IBM WebSphere Security Handbook	http://publib-b.boulder.ibm.com/redbooks.nsf/RedbookAbstracts/sg246573.html?Open

APPENDIX D: CONFIGURATION MANAGEMENT PLANNING RESPONSIBILITY MATRIX

Configuration Management Planning Responsibility Matrix			
Configuration Item	**Responsible Entity**	**Configuration Management Plan [1]**	**Implementation of CI**
Current EPA Standard Technology	OTOP	CI only	System Owner
EPA Target Standard Technology	Shared (OTOP & recommending organization) until adopted as current	CI only	System Owner
EPA Legacy Technology Standard	OTOP (until retired)[2]	CI only[3]	System Owner
Organizational Standard Technology	Organization (in consultation with OTOP)	CI only	System Owner
Organizational or Locally Adopted Technology	Organization (in consultation with OTOP if impacting OTOP managed resources or information systems)	CI only	System Owner
Information System and Components	System Owner	All CIs within system in coordination with above configuration management CIs and processes	System Owner
EPA Standard with Approved Modification	OTOP in coordination with organization for specific modification(s)	CI only	System Owner

[1] *CIs may be grouped into one plan by EPA Technology Type, Technical Reference Model Category or other logical constructs.*
[2] *EPA Organization handles as an Organizational Standard Technology in accordance with waiver conditions if continued via waiver after retirement date.*
[3] *Individual Legacy CIs are withdrawn from any CI Group after retirement date.*

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.4	1/29/2008	Initial draft	Heather Flager	Procedures-CM-Draft_TO62_020_1
1.0	6/29/2009	Incorporated EPA comments	Heather Flager	Procedures-CM-Final_TO62_020_2
1.9	7/24/2010	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_CM_Draft.TO-062_050_1.0
1.9	7/30/2010	TISS Comments and Changes	Charleen Johnson	Procedures_CM_Draft.TO-062_050_1.0
2.0	1/13/2010	TISS Final Draft Review	Charleen Johnson & Mark Hubbard	Procedures_CM_Draft.TO-062_050_1.0
2.1	5/2/2012	SAISO Final Review	Abe Getchell	Procedures_CM_Draft.TO-062_050_1.0
2.2	7/17/2012	Document Review	LaToya Gordon	Procedures_CM_Draft.TO-062_050_1.0