Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Configuration Management (CM) Procedure

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Configuration Management (CM) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

2. SCOPE

These procedures address all United States 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 EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. BACKGROUND

EPA is responsible for ensuring 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 shall meet security requirements by implementing the security controls defined in the NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

This document adopts procedures and standards for the EPA consistent with FIPS Publication 200.

5. AUTHORITY

Additional legal foundations for the Configuration Management Procedure include:

- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.), December 18, 2014
- OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016

- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

6. PROCEDURE

SIO, ISO and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "CM" designator (e.g., CM-2, CM-3) identified for each procedure below corresponds to the NIST- identifier for the Configuration Management control family, as identified in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*.

NIST defines the applicable CM security and privacy baseline controls in NIST 800-53B, Control Baselines for Information Systems and Organizations. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name.

CM-2 – Baseline Configuration

For All Systems:

1) Develop, document, and maintain under configuration control, a current baseline configuration of the system; and
2) Review and update the baseline configuration of the system:
   a) Annually;
   b) When required due to significant changes to the system; and
   c) When system components are installed or upgraded.

CM-2(2) – Baseline Configuration | Automation Support for Accuracy and Currency

For Moderate and High Systems:

1) Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms as specified in the system security plan or configuration management plan.

CM-2(3) – Baseline Configuration | Retention of Previous Configurations

For Moderate and High Systems:

1) Retain one (1) of the previous versions of baseline configurations of the system to support rollback.

CM-2(7) – Baseline Configuration | Configure Systems and Components for High-risk Areas

For Moderate and High Systems:

1) Issue specially configured devices with hardened configurations to individuals traveling to locations that the organization deems to be of significant risk; and
2) Apply the following controls to the systems or components when the individuals return from travel:
   a) Examining the device for signs of physical tampering;
   b) Scanning all files for viruses or malicious content while off network; and
   c) Re-imaging of the resource to the approved baseline image prior to reuse.

CM-3 – Configuration Change Control

For Moderate and High Systems:

1) Determine and document the types of changes to the system that are to be configuration-controlled;
2) Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
3) Document configuration change decisions associated with the system;
4) Implement approved configuration-controlled changes to the system;
5) Retain records of configuration-controlled changes to the system for at least five (5) years;
6) Monitor and review activities associated with configuration-controlled changes to the system; and
7) Coordinate and provide oversight for configuration change control activities through the local Change Advisory Board (CAB) that convenes weekly or on an ad-hoc basis to address emergency changes.

CM-3(1) – Configuration Change Control | Automated Documentation, Notification and Prohibition of Changes

For High Systems:

1) Use automated mechanisms to:
   a) Document proposed changes to the system;
   b) Notify the local CAB of proposed changes to the system and request change approval;
   c) Highlight proposed changes to the system that have not been approved or disapproved within two (2) weeks/ten (10) business days;
   d) Prohibit changes to the system until designated approvals are received;
   e) Document all changes to the system; and

f) Notify the SO, ISO, Information Management Officer (IMO), Information System Security Officer (ISSO), and Configuration Manager when approved changes to the system are completed.

CM-3(2) – Configuration Change Control | Testing, Validation and Documentation of Changes

For Moderate and High Systems:

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

CM-3(4) – Configuration Change Control | Security and Privacy Representatives

For Moderate and High Systems:

1) Require the ISO or ISSO, the Liaison Privacy Official (LPO) and a member of Office of Information Security and Privacy (OISP) to be members of the Enterprise CAB.

CM-3(6) – Configuration Change Control | Cryptography Management

For High Systems:

1) Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: generation, distribution, storage, access and destruction of digital certificates or cryptographic keys; device, data and transmission encryption; and encryption capabilities built into software/hardware.

CM-4 – Impact Analyses

For All Systems:

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

CM-4(1) – Impact Analysis | Separate Test Environments

For High Systems:

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

CM-4(2) – Impact Analysis | Verification of Security Functions

For Moderate and High Systems:

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

CM-5 – Access Restrictions for Change

For All Systems:

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

CM-5(1) – Access Restriction for Change | Automated Access Enforcement and Auditing

For High Systems:

1) Enforce access restrictions using automated mechanisms as defined in the SSP or Change Management Plan and role-based access control; and
2) Automatically generate audit records of the enforcement actions.

CM-6 – Configuration Settings

For All Systems:

1) Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using approved security configuration guides (i.e., vendor or manufacturer procedures) located in the U.S. government repository of publicly available security checklists the NIST National Checklist Program (NCP) and other associated EPA approved policies, procedures, checklists and federal guidance from Office of Management and Budget (OMB) and Department of Homeland Security (DHS). The established settings become part of the systems configuration baseline;
2) Implement the configuration settings;
3) Identify, document, and approve any deviations from established configuration settings for all components of the information system based on risk-accepted operational requirements to include presence of controlled unclassified information (CUI); and
4) Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

CM-6(1) – Configuration Settings | Automated Management, Application, and Verification

For All Systems:

1) Manage, apply, and verify configuration settings for all system components using automated mechanisms defined in the SSP or CMP and manual reviews as necessary.

CM-6(2) – Configuration Settings | Respond to Unauthorized Changes

For High Systems[1]:

1) Take the following actions in response to unauthorized changes to the approved configuration baseline:
   a) Immediately alert the ISO, ISSO, and Configuration Manager. If a security incident is suspected or confirmed, notify the Enterprise Information Service Desk (EISD);
   b) Perform root-cause analysis to determine how the unauthorized changes occurred;
   c) Reconfigure the system to the approved baseline;
   d) Identify and apply lessons learned to prevent future similar issues; and
   e) Require mandatory retraining.

CM-7 – Least Functionality[2]

For All Systems:

1) Configure the system to provide only mission essential capabilities; and
2) Prohibit or restrict the use of the following functions, ports, protocols, and/or services:[3]
   a) Port 20: File Transfer Protocol (FTP) Data Transfer – TCP / SCTP / UDP;
   b) Port 21: File Transfer Protocol (FTP) Control (command) – TCP / SCTP / UDP;
   c) Port 23: Telnet – TCP / UDP;
   d) Port 25: Simple Mail Transfer Protocol (SMTP) – TCP / UDP;
   e) Port 53: Domain Name System (DNS) – TCP / UDP;
   f) Port 80: Hypertext Transfer Protocol (HTTP) – TCP / SCTP / UDP;
   g) Port 110: Post Office Protocol (POP3) – TCP / UDP;
   h) Port 118: Structured Query Language (SQL) Services – TCP / UDP;
   i) Port 137: NetBIOS – TCP / UDP;
   j) Port 143: Internet Message Access Protocol (IMAP) – TCP / UDP;
   k) Port 156: Structured Query Language (SQL) Services – TCP / UDP;
   l) Port 161: Simple Network Management Protocol (SNMP) – TCP / UDP;
   m) Port 194: Internet Relay Chat (IRC) – TCP / UDP;
   n) Port 5060: Session Initiation Protocol (SIP) – TCP / UDP; and
   o) All other ports/protocols not necessary for the system to function.

CM-7(1) – Least Functionality | Periodic Review

For Moderate and High Systems:

1) Review the system vulnerability reports weekly to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and
2) Disable or remove functions, ports, protocols, software and services listed in CM-7.

[1] The EPA CDM provides an automated capability to identify deviations from the approved configuration baselines and provide visibility at the organization's enterprise level. for all information systems. Note that CDM can provide central monitoring but will not automatically update settings. For more information, refer to EPA CDM CONOPS and the EPA Continuous Monitoring Strategic Plan.

[2] For more information, refer to EPA Continuous Monitoring Strategic Plan.

[3] Refer to NIST SP 800-53, Revision 5 for additional guidance on functions, services, including services provided by ISCs or individual components and disabling unused or unnecessary physical and logical ports/protocols.

CM-7(2) – Least Functionality | Prevent Program Execution

For Moderate and High Systems:

1) Prevent program execution in accordance with:
   a) Federal guidance, EPA policy, rules of behavior and/or access agreements regarding software program usage and restrictions; and
   b) Rules authorizing the terms and conditions of software program usage.

CM-7(5) – Least Functionality | Authorized Software — Allow-by-exception

For Moderate and High Systems:

1) Identify all software authorized to execute on the system or system components;
2) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and
3) Review and update the list of authorized software programs annually or when authorized software is added or removed from the list.

CM-8 – System Component Inventory

For All Systems:

1) Develop and document an inventory of system components that:
   a) Accurately reflects the system;
   b) Includes all components within the system;
   c) Does not include duplicate accounting of components or components assigned to any other system;
   d) Is at the level of granularity deemed necessary for tracking and reporting; and
   e) Includes the following information to achieve system component accountability:
      i) Information system/component owner;
      ii) Manufacturer;
      iii) Function;
      iv) Model;
      v) Device type (i.e. server, desktop, appliances, etc);
      vi) Serial number;
      vii) Physical location;
      viii) Software Name and manufacturer;
      ix) Software license information;
      x) Software/firmware version information;
      xi) Operating System version;
      xii) Device name;
      xiii) Media Access Control (MAC) address;
      xiv) Static Internet Protocol (IP) address (IPv4 as necessary and IPv6); and
2) Review and update the system component inventory annually or when authorized changes are made.

CM-8(1) – System Component Inventory | Updates During Installation and Removal[4]

For Moderate and High Systems:

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

CM-8(2) – System Component Inventory | Automated Maintenance

For All Systems:

1) Maintain the currency, completeness, accuracy, and availability of the inventory of system components using automated mechanisms defined in the SSP or the CMP.

CM-8(3) – System Component Inventory | Automated Unauthorized Component Detection

For Moderate and High Systems:

1) Detect the presence of unauthorized hardware, software, and firmware components within the system using an automated mechanism run daily; and
2) Take the following actions when unauthorized components are detected:
   a) Prevent network access or isolate such components;
   b) Analyze the change, and change logs for indications of malicious activity; and
   c) Notify the SA, ISO, ISSO, and the Configuration Manager. If malicious activity is suspected or confirmed, report the incident to EISD.

CM-8(4) – System Component Inventory | Accountability Information

For All Systems

1) Include in the system component inventory information, a means for identifying by role, individuals responsible and accountable for administering those components.

CM-9 – Configuration Management Plan

For Moderate and High Systems:

1) Develop, document, and implement a configuration management plan for the system that:
   a) Addresses roles, responsibilities, and configuration management processes and procedures;
   b) Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
   c) Defines the configuration items for the system and places the configuration items under configuration management;
   d) Is reviewed and approved by the SO and ISO or their designee; and

[4] *For more information, refer to EPA Continuous Monitoring Strategic Plan- Appendix C.*

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

CM-10 – Software Usage Restrictions

For All Systems:

1) Use software and associated documentation in accordance with contract agreements and copyright laws;
2) Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3) Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

CM-11 – User-installed Software

For All Systems:

1) Establish EPA Software Management and Piracy Policy and Procedure, Acceptable Use Policy, User Agreement and/or Rules of Behavior[5] governing the installation of software by users;
2) Enforce software installation policies through the following methods: use of automated mechanism referenced in CM-8(3); and
3) Monitor policy compliance monthly.

CM-12 – Information Location

For All Systems:

1) Identify and document the location of all CUI including but not limited to Confidential Business Information (CBI), Personally Identifiable Information (PII), Sensitive Personally Identifiable Information (SPII), and the specific system components on which the information is processed and stored;
2) Identify and document the users who have access to the system and system components where the information is processed and stored; and
3) Document changes to the location (i.e., system or system components) where the information is processed and stored.

CM-12(1) – Information Location | Automated Tools to Support Information Location

For Moderate and High Systems:

1) Use automated tools to identify all CUI on system components listed in the system inventory per CM-8 to ensure controls are in place to protect organizational information and individual privacy.

[5] *Refer to EPA Information Procedure, Information Security – National Rules of Behavior, CIO 2150-P-21.0*

7. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

8. RELATED INFORMAITON

- CIO 2150-P-08.2, Information Security – Incident Response Procedures, Chief Technology Officer (CTO) Responsibilities in Selected Information Directives: Refer CIO Transmittal No: 15-010, CIO Approval Date: 06/12/2016, Appendix A
- CIO 2123.0-P-01.1, Configuration Management Procedure: Refer CIO Transmittal No: 13-003, CIO Approval Date: 06/10/2016
- EPA Agency Change Management Process (CMP) and Procedures, Version 4.5, 04/08/2014
- NIST SP 800-40, Version 3, Creating a Patch and Vulnerability Management Program, July 2013
- NIST SP 800-70, Revision 4, National Checklists Program for IT Products: Guidelines for Checklists Users and Developers, February 2018
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011
- NIST SP 800-121, Revision 2, Guide to Bluetooth Security, May 2017

9. DEFINITIONS

- **Baseline Configuration** – A set of specifications and attributes for a system or CI within a system, that has been formally reviewed and agreed on at a given point in time and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases and/or changes. [SP 800–128].
- **CMP&P** – created to represent EPA's Agency Change Management Process and Procedures, Version 4.5, 4/8/2014 not to be confused with EPA Procedure, Configuration Management Procedure, CIO 2123.0-P-01.1.
- **Configuration Control** – Process for evaluating change-requests associated with controlling modifications to hardware, firmware, software and documentation to protect the information system against improper modifications before, during and after system implementation.
- **Confidential Business Information (CBI)** – Information which concerns or relates to the trade secrets, processes, operations, style of works, or apparatus, or to the production, sales, shipments, purchases, transfers, identification of customers, inventories, or amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or other organization, or other information of commercial value, the disclosure of which is likely to have the effect of either

impairing the Commission's ability to obtain such information as is necessary to perform its statutory functions, or causing substantial harm to the competitive position of the person, firm, partnership, corporation, or other organization from which the information was obtained, unless the Commission is required by law to disclose such information.

- **Configuration Item (CI)** – An identifiable part of a system (e.g., hardware, software, firmware, documentation or a combination thereof [aggregation]) of Information System Components (ISC) that is a discrete target of configuration control management processes and treated as a single entity in the CMP. 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 EA. 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. [With respect to Security-focused Configuration Management (SecCM), an aggregation of ISCs and treated as a single entity in the CMP.] [NIST SP 800 –128]
- **Configuration Settings** – the configurable security-related parameters of IT products that are part of the information system.
- **Event Driven**[6] – when the information system or its environment of operation changes or the system is compromised or breached; or when the information system may be authorized for ongoing operation on an event-driven basis when pre-defined (trigger) events occur or at the discretion of the AO leveraging the security-related information generated by the continuous monitoring program.
- **Information System Component (ISC)** – A discrete identifiable IT asset that represents a building block of an information system. [NIST SP 800-128]
- **Information System User** – Individual or (system) process acting on behalf of an individual, authorized to access an information system. [With respect to SecCM, an information system user is an individual who uses the information system functions, initiates change requests and assists with functional testing.] [CNSS-4009; NIST SP 800-128].
- **Information Technology (IT) Product** – A system, component, application, etc., that is based upon technology, which is used to electronically process, store or transmit information. [NIST SP 800-128]
- **Personally Identifiable Information (PII)** – Information that can be used to distinguish or trace an individual's identity—such as name, social security number, biometric data records—either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).
- **Security Configuration Checklist** – a series of instructions or procedures for configuring an ISC to meet operational requirements and is sometimes referred to as a lockdown guide, hardening guide, security guide, STIG or benchmark.
- **Security-focused Configuration Management (SecCM)** is used to emphasize the concentration on information security; and is defined as the management and control

[6] *Defined in NIST SP 800-37 Revision 2, RMF Step 6, Monitor Security Controls, Task 6-5, Security Status Reporting; and Appendix F, Security Authorization. Sections F.4, Ongoing Authorization and F.5 Reauthorization*

of configurations for information systems to enable security and facilitate the management of information security risk.

- **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
- **Sensitive PII (SPII)** – A subset of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. At EPA, SPII is defined as social security numbers or comparable identification numbers, biometric data, financial information or medical information associated with an individual. SPII requires additional levels of security controls.
- **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.
- **Significant Change** – a change that is likely to substantively affect the security or privacy posture of a system.
- **Software Inventory Tools** – examples of automated mechanisms that help organizations maintain consistent baseline configurations for information systems.
- **Time Driven** – when the information system is reviewed and authorized for ongoing operation on a time-driven basis, (e.g., weekly, monthly, or quarterly), in accordance with the authorization frequency determined as part of the continuous monitoring strategy.
- **Written (or "in writing")** – to officially document the action or decision, either manually or electronically and includes a signature.

10. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

11. MATERIAL SUPERSEDED

Information Directive: CIO 2150.3-P-05.1 Information Security – Interim Configuration Management Procedures

12. CONTACTS

For further information, please contact the Office of Mission Support, Office of Information Security and Privacy (OISP).

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2023.06.12 08:16:26 -04'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information and Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS & ABBREVIATIONS

AO	Authorizing Official
CAB	Change Advisory Board
CBI	Confidential Business Information
CI	Configuration Item
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management/Manager
CMP	Configuration Management Plan
CMP&P	Change Management Process and Procedures
CSIRC	Computer Security Incident Response Capability
CTO	Chief Technology Officer
CUI	Controlled Unclassified Information
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IMAP	Internet Message Access Protocol
IMO	Information Management Officer
IRC	Internet Relay Chat
ISC	Information System Component
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
POP3	Post Office Protocol 3
OMB	Office of Management and Budget
OISP	Office of Information Security and Privacy
OITO	Office of Information Technology Operations
SCTP	Stream Control Transmission Protocol
SecCM	Security-focused Configuration Management
SI	System and Information Integrity
SIO	Senior Information Official
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
SQL	Structured Query Language
STIG	Standard Technical Implementation Guide
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
U.S.C.	United States Code