Configuration Management Policy		
Directive No: CIO 2123.2	CIO Approval: August 2019	Review Date: August 2021

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

Configuration Management Policy

1. PURPOSE

The purpose of this Policy is to establish an Agency-wide Configuration Management Program and to provide responsibilities, compliance requirements, and overall principles for Configuration and Change Management processes to support information technology management across EPA.

2. SCOPE

This Policy is applicable to all of EPA's Enterprise hardware, software, and applicable documentation that might impact EPA network performance, operations and security. Hardware and software used for specialty or scientific purposes that are disconnected from the EPA network do not fall under the scope of this Policy.

3. AUDIENCE

The primary audience for the Configuration Management Policy includes all EPA personnel in roles that are directly responsible for the configuration, management, oversight, and successful day-to-day operations of EPA Enterprise hardware, software and applicable documentation.

4. BACKGROUND

Information systems are typically dynamic, causing the system state to change frequently as a result of upgrades to hardware, software, firmware or modifications to the surrounding environment in which a system resides. Industry standards, including those issued by the Government Accounting Office (GAO) and the Office of Management and Budget (OMB), and several National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications (SP), stress that information systems (e.g., general support systems, major applications, and minor applications) must document and assess the potential impact that proposed system changes may have on the operational processes and security posture of the system. Information Technology (IT) industry best practices recognize this as an essential aspect of effective system management, as well as being part of the continuous monitoring and maintenance of security accreditation of Federal systems required.

5. AUTHORITY

- Federal Information Security Management Act (P.L. 107-347, Title III), December 2002;
- National Institute of Standards and Technology (NIST) Federal Information Processing

Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004;

- National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006;
- National Institute of Standards and Technology (NIST) Special Publication 800-30, *Risk Management Guide for Information Technology Systems;*
- National Institute of Standards and Technology (NIST) Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems;*
- National Institute of Standards and Technology (NIST) Special Publication 800-40; *Creating a Patch and Vulnerability Management Program;*
- National Institute of Standards and Technology (NIST) Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*;
- National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*;
- National Institute of Standards and Technology (NIST) Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*;
- National Institute of Standards and Technology (NIST) Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*;
- National Institute of Standards and Technology (NIST) Special Publication 800-70, *Security Configuration Checklists Program for IT Products -- Guidance for Checklists Users and Developers;*
- Clinger-Cohen Act in Pub. L. No. 104-208 (Sept. 30, 1996)

6. POLICY

a) EPA Program Offices and Regions must meet or exceed all Federal regulatory policies and procedures which affect Configuration and Change Management processes to be implemented on EPA information technology assets.

b) Each Program Office and Region must document, implement, and maintain Configuration and Change Management processes, in collaboration with the Office of Mission Support, Office of Information Technology Operations. These processes must include the following:

(1) Documenting and maintaining the configuration baseline(s) applicable to the deployed system;

(2) Effectively managing and tracking all system configuration and associated document changes, as well as the integrity, availability and maintainability of the system;

(3) Effectively planning to ensure the ability to reverse a deployment or implementation; and

(4) Effectively tracking all system changes made, including installation of patches, to hardware, software, firmware, and documentation, through development,

approval, testing, and controlled implementation of changes delivered into production environments.

c) Configuration and Change Management processes must incorporate applicable industry best practices, which support optimum production system availability and effective system management. These practices include:

(1) Using standardized documented methods, processes, and procedures;

(2) Effectively tracking and communicating all system changes made to hardware, software, firmware, and documentation, through planning, approving, notifying, developing, testing, scheduling, and managing the implementation of changes;

(3) Making effective risk-based decisions to maintain each system's mission capability, authorized security posture and minimized risk; and

(4) Maximizing EPA resources.

d) Program Offices and Regions that maintain a network infrastructure connected to the EPA network must establish Change Advisory Boards (CAB) as appropriate to ensure changes to the EPA infrastructure are reviewed and processed in accordance with established EPA Configuration and Change Management processes and procedures.

e) Each Program Office and Region must utilize a Configuration Management Database (CMDB) that contains and tracks relevant information about configuration items, their attributes, baselines, documentation, changes, and relationships. Existing or new systems may fulfill this requirement. The Office of Mission Support, Office of Information Technology Operations (OMS-OITO) will establish an OITO-wide standard to which all existing and new CMDBs may conform.

f) Any changes to portions of EPA's IT environments that might impact network security, performance, or operations must be recorded in a central tracking application and database. These include changes to portions of EPA's IT environments, including network, LAN, WAN, telecommunications, mainframe, hosting, and servers. OITO has provided specific guidance as to the types of changes that must be recorded. For more information refer to the Agency Change Management Process and Procedures, under Related Documents.

7. ROLES AND RESPONSIBILITIES

Required roles and responsibilities may be fulfilled by one or more individuals.

EPA Chief Information Officer (CIO) is responsible for:

- Approving and issuing policies, procedures and guidance for implementing and coordinating the EPA Configuration Management Program;
- Implementing the EPA Configuration and Change Management Programs, as appropriate;
- Directing, monitoring, and enforcing implementation and maintenance of, and compliance with, the EPA Configuration and Change Management Programs; and

- Periodically testing and evaluating IT components to determine effectiveness and compliance with the EPA Configuration and Change Management Programs.

Change Advisory Board (CAB) is responsible for:

- Provide enterprise risk management, communication management and process compliance management to the change process environment;
- Review/Approve changes and ensure changes to EPA infrastructure or contracted EPA systems are reviewed and processed in accordance with established Change Management processes and procedures;
- Establishing a secure and sound configuration management framework ensuring definition and maintenance of configuration baselines and the identification, management and tracking of associated hardware, software and documentation configuration items for each EPA system;
- Ensuring all changes to configuration items adhere to EPA policy and are documented, tested, and approved. This includes ensuring changes are evaluated to determine the impact to system security before implementation;
- Ensuring that EPA Configuration and Change Management process documents are maintained as a Configuration Item (CI) component and placed under configuration management control; and
- Reporting on the effectiveness of the Configuration and Change Management activities to executive leadership.

Director of Information Technology Operations is responsible for:

- Providing procedures, standards, and guidance to senior level managers in support of the Agency's Configuration Management Policy;
- Instituting change management processes; and
- Providing a Change Management database.

Office of Mission Support, Office of Information Technology Operations (OMS-OITO) is responsible for:

- Addressing questions and concerns regarding interpretation of this policy and accompanying procedures;
- Collaborating with EPA Program Offices and Regions in the development of Configuration and Change Management processes; and
- Establishing and maintaining enterprise configuration management capabilities.

Program Offices and Regions are responsible for maintaining explicit control of changes to the business system under their authority.

Senior Information Officials (SIOs) are responsible for ensuring that their office is in compliance with EPA Configuration Management Policy and Procedures.

8. RELATED INFORMATION

For more information on this procedure, please contact the Office of Mission Support, Office of Technology Operations, Mission Investment Solutions Division.

9. DEFINITIONS

Change Advisory Board is a group of people responsible for evaluating and approving or disapproving proposed changes to configuration items, and for ensuring implementation of approved changes.
Change Management is a critical discipline that controls and communicates the changes occurring in the IT environment.
Configuration Baseline is a configuration information formally designated at a specific time during a product's or product component's life. Configuration baselines, plus approved changes from those baselines, constitute the current configuration information.
Configuration Item is an aggregation of work products that is designated for configuration management and treated as a single entity in the configuration management process. This aggregation consists of all required components: hardware, software, and other items that comprise a baseline.
Configuration Item Attributes are descriptive characteristics of configuration items (CI), such as a make or model number, version number, supplier, purchase contract number, release number, data format, role or relationship, held in the Configuration Management database (CMDB).
Configuration Management is a discipline applying technical and administrative direction and surveillance to (1) identify and document the functional and physical characteristics of a configuration item, (2) control changes to those characteristics, (3) record and report change processing and implementation status, and (4) verify compliance with specified requirements.
Configuration Management Database is a Database which stores attributes of CIs and relationships with other CIs.
Information Technology Assets are EPA's hardware, software and applicable documentation.

10. WAIVERS

No waivers will be accepted from the requirements of this policy.

11. MATERIAL SUPERSEDED

Configuration Management Policy, CIO Transmittal No.: 12-001, EPA Classification No.: CIO 2123.0, CIO Approval Date: 03/27/2012

12. CONTACTS

For more information on this procedure, please contact the Office of Mission Support, Office of Technology Operations, Mission Investment Solutions Division.

Configuration Management Policy		
Directive No: CIO 2123.2	CIO Approval: August 2019	Review Date: August 2021

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2019.08.19 13:15:02 -04'00'

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