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

Configuration Management Procedure

1. PURPOSE

The purpose of this procedure is to describe the process EPA Program Offices and Regions must follow to comply with the Environmental Protection Agency's (EPA or Agency) Configuration Management Policy.

2. SCOPE

This Procedure 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 Procedure.

3. AUDIENCE

The primary audience for the Configuration Management Procedure 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

Configuration Management is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process to manage and control the baselines and configurations of an organization's Enterprise hardware, software, and applicable documentation. 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. IT industry best practices recognize configuration management as an essential aspect of effective system management.

Configuration Management consists of 4 main tasks:

- Identification – this is the specification of all IT components (configuration items) and their inclusion in a Configuration Management Database (CMDB)
- Control – this is the management of each configuration item, specifying who is authorized to 'change' it

- Status – this is the recording of the current condition of all configuration items in the CMDB, and the maintenance of this information
- Verification – this is the review and audit of the information contained in the CMDB to ensure it is accurate

A configuration item is an IT asset or a combination of IT assets that may depend on and have relationships with other IT processes. Configuration Management involves tracking all of the individual configuration items in an IT system in a CMDB. Information contained in the CMDB includes:

- Hardware
- Software
- Documentation
- Personnel

The CMDB can be comprised of a multitude of different types of configuration items, each containing various attributes, and is used to document configuration item relationships and track their configuration. A configuration item will have attributes which may be hierarchical and relationships that will be assigned by the Configuration Manager in the CMDB. Appendix A lists some attributes that can be used to assist with identifying the type and level of data a Program Office or Region may consider useful.

5. AUTHORITY

EPA's Configuration Management Policy, June 10, 2013

6. PROCEDURE

In accordance with EPA's Configuration Management Policy, Program Offices and Regions, in collaboration with the Office of Mission Support, Office of Information Technology Operations, must document, implement, and maintain configuration management processes.

Configuration Management processes include properly identifying configuration items, controlling changes, and recording the change implementation status of the physical and functional characteristics of the IT infrastructure. This ensures the overall integrity of the EPA Enterprise. This process is accomplished through implementation of the five tenets of Configuration Management:

- Configuration Planning and Management
- Configuration Identification
- Configuration Change Management
- Configuration Status Accounting
- Configuration Verification and Audits

CONFIGURATION PLANNING AND MANAGEMENT

Program Offices and Regions must develop a strategy to define the scope and objectives of a configuration management process as well as identify configuration items that shall be

tracked within the CMDB. They should also collectively decide, in collaboration with the Office of Mission Support, Office of Information Technology Operations, which attributes of configuration items are necessary for distinguishing between configuration items. When deciding what level of attribute to record it is important to remember the frequency at which the data will be used, by whom it will be used, and what value can be placed on it, together with the cost and effort involved in maintaining it.

CONFIGURATION IDENTIFICATION

Program Offices and Regions must identify candidate system components, items, and data that will be placed under configuration control and management. This encompasses the following:

- Identification of applicable configuration items
- Establishment of baselines for control; maintenance of versions and revisions Identification of approved configuration documentation of the physical and functional characteristics of the item or system
- Creation of records in the CMDB
- Provision of documentation for configuration management and external audits
- Management of configuration item document library in CMBD

Configuration items should be managed throughout the system development life cycle in order to establish and maintain the integrity of the IT product or service. Appendix B lists what Program Offices and Regions can classify as configuration items for information systems.

CONFIGURATION CHANGE MANAGEMENT

Program Offices and Regions must implement a controlled change process and provide tailored methods and standard operating procedures for effectively planning, recording, controlling, and validating product requirements and data that contain the requirements. Tailoring will depend on the organization and the level of control or complexity needed.

Configuration management control is accomplished by utilizing the CMDB, a centralized configuration management database, or a series of databases that provide central, logical access to configuration data, containing relevant information such as the configuration items and their attributes, baselines, documentation, changes, and relationships. Requests for Changes must be stored in the CMDB.

CONFIGURATION STATUS ACCOUNTING

The CMDB tool must be used to track submitted Requests for Changes. The objectives of the system are to provide enhanced coordination, visibility, and accountability. Records describing configuration items must be established and maintained in the CMDB. The tool must assign a unique identifier to each Request for Change and maintain a repository of all change requests.

Program Offices and Regions must record actions in sufficient detail that the content and status of each Configuration Item is known and previous versions can be recovered.

Organizations must maintain product description records, configuration verification records, change status records, and history of change approvals.

The CMDB must contain relevant information about configuration items, their attributes, baselines, documentation, changes, and relationships. The recording of changes must include:

- The reason for the changes
- If a proposed change to the configuration item is accepted, a schedule for incorporating the change into the configuration item and other affected areas
- Indication that changed configuration items have been released only after review and approval of configuration changes. Changes are not official until they are approved

CONFIGURATION VERIFICATION AND AUDITS

Configuration auditing must be performed by Program Offices and Regions to verify the integrity of the processes, systems, items, and baselines under Configuration Management control. The Configuration Manager conducts these audits to ensure baseline compliance of the configured assets' hardware, software, and controlled documentation with established requirements, specifications, and functional parameters. Change control processes are also subject to Configuration Management Audits.

Additionally, Configuration Management Audits must be used to ensure the accuracy of the CMDB; address the effectiveness of the Change Advisory Board; determine the accuracy and completeness of Configuration Management processes; verify data and documentation; and ensure project compliance with requirements, standards, and conventions.

All audit records and respective deficiencies must be placed into the CMDB, which shall be used to track corresponding action items, suspense dates, and close-out activities. The Configuration Manager can decide whether these attributes need to be tracked within the CMDB since he/she is responsible for conducting periodic audits. The CMDB must be used to maintain a historical file of all audit information throughout the applicable life cycle. The Configuration Manager must conduct its audits on a periodic basis following a defined audit sequence. The Configuration Manager must have the responsibility to initiate the audit sequence and oversee its implementation.

7. ROLES AND RESPONSIBILITIES

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

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.

Change Coordinator is responsible for:

- Coordinating and facilitating CAB meetings;
- Documenting and distributing CAB meeting minutes, decisions and actions;
- Reviewing proposed Requests for Changes;
- Preparing and distributing implementation schedules for all approved changes;
- Providing immediate disposition of directed or emergency changes, without going through the mechanism of change control;
- Assisting with Change Post Implementation Reviews;
- Collecting, collating and reporting change management metrics; and
- Executing tasks delegated by the CAB Chairperson.

CAB Chairperson is responsible for:

- Managing and maintaining the Change Control process;
- Ensuring compliance to the Change Control process;
- Tabling Requests for Changes for CAB meetings;
- Determining CAB meeting participants based on the nature of the Requests for Changes;
- Chairing the CAB;
- Convening meetings to consider emergency Requests for Changes; and
- Acting as a central point of contact and escalation point for change management issues.

Configuration Manager is responsible for:

- Overall responsibility and authority for the Configuration Management process;
- Handling all Configuration Management issues involving management and oversight of requirements; architectural integrity; site configurations; version control; hardware/software development; interoperability; status accounting; change disposition; auditing; and, adherence to established standards and guidance;
- Ensuring that proposed changes are executed within a disciplined process, giving adequate consideration to the technical, programmatic, security, and schedule impacts of the proposed changes;
- Conducting audit reviews;
- Initiating the audit sequence and overseeing its implementation; and

- Assigning attributes to configuration items.

Change Implementers are responsible for:

- Testing requested changes;
- Implementing changes;
- Reversing changes;
- Entering configuration status accounting information; and
- Responding to inquiries regarding changes.

Change Requestor is responsible for originating a Request for Change.

Director of Office 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 approval system for EPA (i.e., CDMB, a change approval and tracking application and database).

Office Mission Support, Office of Information Technology Operations (OMS-OITO) is responsible for addressing questions and concerns regarding interpretation of these procedures.

Program Offices and Regions are responsible for maintaining explicit control of changes to the business systems 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

- Capability Maturity Model® Integration for Development, Version 1.3, November 2010 Carnegie Mellon, Software Engineering Institute
- Electronic Industries Alliance 649, National Consensus Standard for Configuration Management, August 1998
- National Institute of Standards and Technology (NIST) Special Publication 800-12 (An Introduction to Computer Security; the NIST Handbook), October 1995
- Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Systems, November 2000
- Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Internal Control, June 1995
- National Institute of Standards and Technology (NIST) Special Publication 800-53 (*Recommended Security Controls for Federal Information Systems), May 2010*
- EPA System Life Cycle Management Policy, CIO 2121.1, September 21, 2012
- EPA Information Security Policy, CIO 2150.3, August 6, 2012
- Office of Management and Budget (OMB) Memorandum M-07-18, Ensuring New Acquisitions
- Include Common Security Configurations, June 1, 2007

- Office of Management and Budget (OMB) Memorandum M-08-22, Guidance on the Federal Desktop Core Configuration (FDCC), August 11, 2008

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 Audit is an audit conducted to verify that a configuration item, or a collection of configuration items that make up a baseline, conforms to a specified standard or requirement.

Configuration Baseline is 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 Control is an element of configuration management consisting of: the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification.

Configuration Identification is an element of configuration management consisting of: selecting the configuration items for a product, assigning unique identifiers to them, and recording their functional and physical characteristics in technical documentation.

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 fundamentally the science of tracking the exact state of the overall IT environment at any point in time. It 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.

Configuration Status Accounting is an element of configuration management consisting of the recording and reporting of information needed to manage a configuration effectively. This information includes a listing of the approved configuration identification, the status of proposed changes to the configuration, and the implementation status of approved changes.

10. WAIVERS

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

11. MATERIAL SUPERSEDED

Configuration Management Procedure, CIO 2123.0-P-01.2

12. CONTACTS

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

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2022.09.13 09:06:48 -04'00'

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

APPENDIX A: CONFIGURATION ITEM ATTRIBUTES

Location	Physical location of the Configuration Item (Region/Program, Building, Floor, Section, Room, etc.)
Model / Hardware + Software Configuration	Details of specific Model purchased, software version, hardware manufacturer specifications, specific HW and SW Configuration Image applied, etc.
Source code	Name, Owner, Version, Date, Location, etc.
Software Licenses	Software agreement(s) details
Documentation	Name, Author, Version, Date, Location, etc.
Status	Ordered, Delivered, Installed, Repair, Stolen, Decommissioned, Disposed, etc.
Maintenance Contract	Bronze, Silver, Gold, Platinum
Incident Records	Open and Closed, Historical and Present
Problem Records	Open and Closed, Historical and Present
Change Records	Planned and Completed, Future and Historical
User associated with the configuration item	Name, Job Function/Title, Telephone, Contact details, etc.
Relationships with other configuration items	Both Parent & Child

APPENDIX B: CONFIGURATION ITEM IDENTIFICATION

Goal	Include Configuration Items	Which will make it possible to:
To improve impact assessments of IT infrastructure changes to IT services	Demonstrate relationships across IT components (e.g. hosting, networking, databases, etc.) that comprise the IT service.	Determine how a change to one device (e.g. server) might affect other systems in an IT service.
To track, analyze and report on changes made to the agency's IT infrastructure	May or will have a HQ or Agency-wide impact. These types of changes include desktop solutions, mobile devices, hardware, software, network environments, middleware, firmware and systems managed by OMS, Office of Information Technology Operations or changes made at the Regional level that may have an impact beyond the region.	Track Configuration Items that changed, number of changes made, and when the changes were made.