U.S Department of Housing and Urban Development (HUD)

Secure Configuration Management Policy

HUD Handbook 3251.1

July 2023

DOCUMENT CHANGE HISTORY

Issue	Date	Pages Affected	Description
Version 1.0	Nov. 2022	Various	Updates and replaces the Secure Configuration Management Directive
Final Policy 1.0	February 2023	Various	Revisions incorporated based on OCIO organizational review and feedback. Submission into clearance process.
Version 1.0	March 2023	Title page	Completed OCIO Clearance
Version 1.0	May 2023	Various	Format, grammatical, and minor revisions for clarity incorporated from Departmental Clearance comments. Final version 1.0.

TABLE OF CONTENTS

1.0 Introduction

Secure configurations for HUD systems and associated components[1] build on the general concepts, processes, and activities of configuration management and focus on the established security requirements of the organization and systems. Secure configurations are designed to reduce and manage risk and are achieved though the identification of configuration management resources, using approved, standard hardware and software, applying secure configuration settings of information technology (IT) products (e.g., operating systems, databases, etc.), implementing current software versions, maintaining patches, and implementing endpoint protection throughout the system life cycle.

Managing system configurations is a minimum security requirement identified in FIPS 200[2] and the controls that support this requirement are defined in NIST SP 800-53[3]. NIST SP 128[4] provides guidance on the security aspects of configuration management. To comply with Federal regulations, policies, guidance, and memorandums, HUD has established the Secure Configuration Management (SecCM) Policy to provide guidelines for managing and administrating the security of HUD systems and associated environments of operation.

2.0 Purpose

The purpose of this policy is to establish secure configuration requirements for all HUD information systems, including internal, external, and service-oriented (e.g. cloud) systems and associated environments. This policy outlines the identification of secure baselines, handling of configuration deviations, configuration monitoring, and approved changes to information system configurations. Further, this policy stipulates the identification of resources needed to address the life cycle configuration management requirements for all HUD systems.

Controlling vulnerabilities and reducing threats via implementation of a robust secure configuration management policy is a critical part of HUD's overall risk management process since many vulnerabilities can be traced to software flaws and misconfigurations of system components. Consequently, effective implementation of this policy will maximize security and minimize system vulnerabilities and the potential risk of unauthorized access to HUD information and technology.

3.0 Applicability

The Secure Configuration Management (SecCM) Policy applies to all "HUD entities," their employees, and third parties (such as consultants, vendors, and contractors), that use or access any HUD Information Technology resource and are assigned roles and responsibilities associated with HUD information and business systems life cycle management requirements.

[1] System components include mainframes, workstations, servers (e.g., database, electronic mail, authentication, Web, proxy, file, domain name), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.
[2] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems, Federal Information Processing Standards Publication (FIPS) 200
[3] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Control for Information Systems and Organizations
[4] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-128, Guide for Security-Focused Configuration Management of Information Systems

The SecCM policy applies to:

- All major systems and applications, non-major applications, web applications, general support systems (GSS) and IT services;
- Includes both internal and external systems and applications;
- Includes systems and applications developed and operated on COTS, GOTS, and FedRAMP cloud solutions (IaaS, PaaS, SaaS, etc.);
- Includes Government Owned / Contractor Operated systems and applications; and
- System baseline configurations and revisions that include business applications, operational environments, interfaces, hardware, software, tools, and documentation.

Within HUD, the application of secure configurations applies to authorized information systems that are owned and/or operated by or operated on behalf of HUD.

4.0 Rescission

The Secure Configuration Management Policy rescinds the Secure Configuration Management Directive, dated November 2021. This document will be reviewed on an annual basis and rescission information will be updated as necessary.

5.0 Effective Implementation Date

This policy is effective immediately upon the date of approval.

6.0 Authority

The Federal Information Security Modernization Act of 2014, Public Law number 113-283, provides the Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for the Department, including hardware, software, security and business re-engineering. OMB Memo M-07-18, June 1, 2007, SUBJECT: Ensuring New Acquisition Include Common Security Configurations[5], requires agencies to ensure that new acquisitions include "common security configurations and information technology providers certify their products operate effectively using these configurations." Furthermore, the Federal Acquisition Regulation (FAR), Part 39 Acquisition of Information Technology[6], Subpart 39.101 Policy, confirms that when "acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated."

[5] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2007/m07-18.pdf
[6] https://www.acquisition.gov/far/part-39

7.0 Secure Configurations

Establishing and managing secure configurations requires an investment in time and resources throughout the system's life cycles. This includes managing patches, fixes, and updates, as well as all system modifications required to addresses business requirement changes and modernization efforts. As potential changes to systems are assessed and implemented, baseline configurations must be tested and updated, specific configuration settings confirmed, and configuration items tracked, verified, and reported. Therefore, secure configuration management is a continuous activity that, once incorporated into IT management processes, must be addressed throughout the system life cycle.

The HUD SecCM policy requires that Information Technology (IT) products and systems are inventoried and configured in compliance with IT security policies, standards, and procedures and must include planning and management, resource identification, configuration identification, change management, risk identification and management, status accounting, configuration verification and audit, and information/data management. These requirements apply to all systems and applications and must align with the HUD Project Planning and Management (PPM) life cycle[7] and project types[8]. HUD shall maintain secure configurations by adhering to the configuration management requirements for planning, identifying, maintaining, and monitoring configurations of a system that includes considering business and security impact during the initial approval of a systems configurations, evaluating changes requested to a system's configuration, and documenting all changes made to a system throughout its life cycle.

The following secure configuration standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with the following standards:

7.1 Configuration Management (CM) Resources and Metrics shall

- Be established and maintained using a disciplined approach for ensuring adequate security and limiting risk. This begins in the planning phase for development projects with the identification of configuration management requirements, resources and performance metrics that are used to establish, monitor and ensure compliance with HUD IT Security, Software Configuration Management (SCM) Change Management, Enterprise Patch Management, Configuration Change Management Board (CCMB), IT Project Planning and Management (PPM), and Risk Management policies[9], procedures, and associated templates.

- Identify configuration management resources at the level necessary to achieve adequate configuration management control, security, risk avoidance, business functionality, and service

[7] PPM V2.0 Home Page is available at https://www.hud.gov/program_offices/cio/ppm

[8] PPM V2.0 Project Type Guides and Tools (https://www.hud.gov/program_offices/cio/ppm/PPMV20Guides)

[9] OCIO policies are available at https://www.hud.gov/program_offices/administration/hudclips/handbooks/cio

requirements. These resources must include, at a minimum, a configuration manager. Additional CM resources should be identified based on the size and complexity of the system. CM resource requirements should also include targeted and awareness-level configuration management training for key staff with essential CM responsibilities.

- Include all CM resource requirements in HUD's Investment Planning process and further refined as projects advance through the PPM stages and control gates and into operations and maintenance (O&M).

- Identify CM metrics that align and comply with established policy and procedures to ensure the ability to gather quantitative evidence that the program is meeting its stated goals and monitored to identify opportunities to improve secure configuration management program and processes in general.

7.2 Configuration Management Plans shall

- Adhere to common secure configurations that are established to identify recognized and standardized secure configurations that are applied to configuration items. HUD's common secure configurations are derived from established federal, organization, or industry specifications ((the National Checklist Program contains references to common secure configurations such as the United States Government Configuration Baseline (USGCB), Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) Benchmarks, etc.).

- Develop, document, and implement a configuration management plan that establishes and defines the system configuration management process and associated activities for identifying configuration items and for developing, reviewing, approving, and implementing a secure baseline configuration that will be managed throughout the system life cycle.

- Ensure that each system configuration management plan aligns with HUD software configuration management, Enterprise Patch Management, Change Management, and PPM policies and procedures.

- Ensure that all IT systems and applications comply with established CCMB approved platform standards and obtain prior CCMB approval for any proposed new product standard before using any HUD resources to acquire the product.

- Ensure that all IT systems and applications do not present risk to HUD by using components that are End-of-Life (EOL) or End-of-Support (EOS) and maintain software according to HUD established standards (i.e. the " N-1" standard[10]).

[10] N-1 standard refers to maintaining components at a level that is one version behind the current version or "[current version commercially available] minus [one version]"

- Identify the configuration manager or CM point of contact responsible for management of the CM plan, as well as all other configuration management roles, responsibilities, and configuration management processes and procedures that comply with HUD IT policies.

- Be protected from unauthorized disclosure or modification.

7.3 Baseline Configurations shall

- Be developed, documented, and maintained under configuration management, a current baseline configuration for each information system and application. The approved baseline configuration for a system or application and associated CIs shall represent the most secure state consistent with operational requirements and constraints[11].

- Ensure the documentation of a baseline configuration and configuration settings will include[12]:
  - IT system components (Hardware, software, databases, etc.)
  - Operating system and application features (enabling or disabling depending on the specific feature, setting specific parameters, etc.).
  - Authentication controls (e.g., password length, use of special characters, minimum password age, multifactor authentication/use of tokens).
  - Access controls (e.g., controlling permissions to files, directories, registry keys, and restricting user activities such as modifying system logs or installing applications).
  - Methods of remote access (e.g., SSL, VPN, SSH, IPSEC).
  - Services (e.g., automatic updates) and ports (e.g., DNS over port 53).
  - System settings (e.g., session timeouts, number of remote connections, session lock).
  - Network protocols (e.g., NetBIOS, IPv6), network interfaces (e.g., Bluetooth, IEEE 802.11, infrared), and network protections (e.g., TLS, IPSEC).
- Ensure baselines will adhere to least functionality practices to help prevent security vulnerabilities. Least functionality is carried out by approving and implementing only the essential capabilities and needs of an information system and denying unnecessary settings, and shall include:
  - Review the information system quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services.

[11] As defined in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (available on https://csrc.nist.gov/publications/sp800), the baseline configuration is a documented set of specifications for information system, or the configuration items (CI) within a system, that have been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

[12] The items listed are not meant to be exhaustive as each system will differ.

- Disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.

- Prevent program execution in accordance with policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.

- Prevent system software end-of-life (EOL) and end-of-service (EOS) by maintaining current software version standard (i.e. N-1).

- Prevent software programs not authorized to execute on information systems.

- Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.

- Monitor HUD's list of unauthorized software.

- Help determine a system's requirements and capabilities, by referencing and documenting stack requirements, requirements specification, and requirements traceability matrix[13].

- Be reviewed and updated as required by the IT Security and Privacy Control Catalog[14].

- Identify, standardize, and establish common secure baseline benchmarks and configuration items (CIs) of a system. Reference common secure configurations, such as the National Checklist Program Repository, Defense Information Systems Agency (DISA) Security Technical Information Guides (STIGs), Center for Internet Security (CIS) benchmarks, United States Government Configuration Baseline (USGCB), HUD approved standard images and templates, and vendor provided secure settings as a basis to establish and approve secure configurations of a system. If a benchmark checklist or settings is not available for reference, one will be directed by the TRC for development.

- When the configuration baseline is established and approved in accordance with HUD IT Security and Secure CM policies, the baseline is documented and retained within the CCMB centralized, designated location and associated monitoring tools as applicable. All General Support Systems (GSS) and Major Applications must have specific configuration management plans. All other systems may fall under the enterprise configuration management plan, as determined by the TRC and monitored by the CCMB.

- Be monitored for 30 days after a system or application has been successfully approved and released into production, to ensure the established system requirements and configurations are adequate. The CCMB is notified 30 days after release by the System Owner or IT Project Manager or Program Manager that the system is operating as intended.

[13] More information on this process can be found on the Project Planning and Management (PPM) website, available at https://www.hud.gov/program_offices/cio/ppm

[14] Available under the Documents heading on the Security Template and Document Library website (http://hudatwork.hud.gov/HUD/cio/po/i/it/security/templates)

- Be reviewed and revised as a result of an approved and successfully implemented Request for Change[15] and as an integral part of information system component installations, patches, and upgrades.

7.4 Configuration Change Control

Configuration change control is vital in tracking and managing all changes to configuration baselines, configuration items, and configuration settings of a system. When updates are needed to a systems baseline configuration and CIs due to version upgrades, patches, new qualifications, updated requirements, etc., such requests for change shall:

- Proceed through the change management process that is coordinated and overseen by the CCMB as required by the Change Management Policy, HUD Handbook 3253.1. The CCMB procedures for governing changes to system baseline configurations employs a formal process for identifying, proposing, reviewing, analyzing, testing, and approving all changes to the baseline prior to implementation. All changes to a baseline must be documented within the appropriate system and configuration documentation (e.g., configuration management plans, system component inventories, technical specification and design documentation, system security documentation, etc.).

- Ensure that proposed configuration changes to any information system are tested and analyzed with consideration to risk, performance, cost, and schedule. This resulting information is documented using a Request for Change[16] template and submitted to the CCMB for disposition.

- Ensure approved configuration change requests for information systems are tracked from submission, CCMB determination, testing, and implementation. Once successfully implemented, confirmation is provided to the CCMB and the system baseline documentation is revised to reflect configuration changes to the system.

- Ensure information system change request documentation is routinely reviewed and audited to ensure baseline information is monitored for potential security risks or vulnerabilities and associated documentation is revised accurately and. At a minimum, all systems and applications will review baseline configurations annually and throughout the system life cycle.

- Monitor and perform timely application of appropriate patches and upgrades, security testing, monitoring of event logs, and backups of data and operating system files to ensure maintenance of secure configurations.

[15] HUD Handbook 3253.1, Change Management Policy, August 2022 and HUD Handbook 3254.1, Enterprise Patch Management Policy, August 2022 (available at https://www.hud.gov/program_offices/administration/hudclips/handbooks/cio)

[16] The Request for Change template and instructions are available at http://hudatwork.hud.gov/HUD/cio/po/i/it/sd/devlife/def/CCMB/ccmb

- Perform timely remediation of identified vulnerabilities and Plan of Action and Milestones (POA&Ms) related to misconfigurations.

- Maintain configuration baselines, standard images, and templates in a central location for reference.

7.5 Testing Baseline Configurations Settings

- To ensure secure baseline settings are achieved and implemented, resources must be designated to test, validate, and document the configuration baseline settings during the PPM process execution and control phase.

- During testing, the baseline configuration and common configuration settings are reviewed and assessed for security and risk impact, as well as tested and approved prior to implementation in accordance with HUD's security policy procedures. Once established, the baseline configuration is used as a reference for future builds, releases, and/or changes and will be available from the Configuration Control Management Board (CCMB).

7.6 Configuration Deviations

- Deviations to common secure configurations are identified when systems or applications diverge from secure configurations and settings and can in turn pose a security risk to HUDs infrastructure. Deviations found during system testing, Continuous Diagnostics and Monitoring (CDM) scans and discovery, or other security tool scans, must be examined individually and either resolved or documented as a deviation from, or exception to, the established common secure configurations.

- The establishment of secure configurations for all systems is prioritized based on system impact, risk assessments, and organizational value. When situations occur in which the baseline configuration of a system conflicts with another, HUD will employee configuration prioritization to ensure critical HUD systems are not compromised by the configurations of less critical systems and applications. The following prioritization criteria is considered:

    - System Impact Level – Secure configurations in system with a high or moderate security impact level has priority over systems with a low security impact level
    - Risk assessments – System risk assessments that presents the least impact on security and organizational risk will have higher priority over system with higher impact.
    - Vulnerability scanning – Vulnerability scan results are considered to identify the system that is the most vulnerable. This can include the Common Vulnerability Scoring System (CVSS) scores.
    - Degree of penetration – The degree of penetration represents the extent to which the same product is deployed within an information technology environment. For example, if an organization uses a specific operating system on 95 percent of its workstations, it may obtain the most immediate value by planning and deploying secure configurations for that operating system. Other IT products or CIs can be targeted afterwards.

- When conflicts between applications and secure configurations cannot be resolved, deviations are documented and submitted to the configuration change control process for review and approval by the (CCMB process as appropriate. All deviations from common secure configurations must be justified and recorded using the Request for Change (RFC) template. The deviation request must include appropriate security/risk assessments, business impact analysis, resource analysis, and testing results. Configuration deviations that are expected to require additional configuration management resources and resource estimates should be included in the completed analysis and include an explanation of any compensatory security or other measures implemented to mitigate the risk associated with the deviation.

- The deviation request is only approved if the assessment results presented within the request are within an agreed upon level of risk acceptance that is acceptable by both the system owner and the appropriate Information System Security Officer (ISSO) and approved by the Configuration Change Management Board (CCMB). The agreed level of risk acceptance along with leadership sign off will determine if the system will be allowed to be implemented or continue to operate within the HUD environment[17].

7.7 Configuration Monitoring

- Configuration monitoring involves assessing and reporting the level of compliance a system or application has with the established baseline configuration, CIs, and standards. HUD CM resources use CDM and other security tools as the automated monitoring resource to identify misconfigurations, undiscovered or undocumented system components, vulnerabilities, and unauthorized changes, all of which, if not addressed, can cause increased risk and exposure. HUD CM resources should implement and utilize Security Content Automation Protocol (SCAP) validated tools and other resources, such as the National Vulnerability Database (NVB)[18], for the identification of vulnerabilities. All misconfigurations or related vulnerabilities discovered during security scans are reported to the IT Project or Program Manager (ITPM), System Owner (SO), and Information System Security Officer (ISSO) for mitigation. HUD systems and applications will comply with Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive 22-01, Reducing the Significant Risk of Known Exploited Vulnerabilities (BOD 22-01).[19]

- Configuration examination techniques recommended for HUD systems include the following:
  - Scanning to discover components not recorded in the inventory or identify disparities between the approved baseline configuration and the actual configuration for a system;

[17] It is important to note that deviation request approval does not waive requirements set forth in HUD Handbook 2400.25, IT Security Policy, and the HUD IT Security Catalog.

[18] The NVD is available on the National Institute of Standards and Technology (NIST) website: https://nvd.nist.gov/

[19] BOD 22-01 is available at https://www.cisa.gov/binding-operational-directive-22-01. This directive establishes a CISA-managed catalog of known exploited vulnerabilities that carry significant risk to the federal enterprise https://cisa.gov/known-exploited-vulnerabilities and establishes requirements for agencies to remediate any such vulnerabilities included in the catalog.

- Querying audit records and monitoring system logs to identify unauthorized configuration changes;
- Running system integrity checks to verify that baseline configurations have not been changed; and
- Reviewing configuration change control records (including security impact analyses) to verify conformance with HUD CM policies and procedures.

- Changes detected as a result of the above monitoring activities are reconciled with approved changes to determine the:
  - Who made the change;
  - Whether the change occurred in a scheduled maintenance window;
  - Whether the change matches a previously detected and approved change; and
  - Whether the change corresponds with an approved change request, service or help desk ticket, or product release.

- Unauthorized changes detected during CM monitoring activities are analyzed to determine the reason(s) that an unauthorized change occurred and may include:
  - Accidental or unintentional changes;
  - Malicious intent/attacks;
  - Errors made when changes are implemented; or
  - A delay between introducing the change and updating the inventory and baseline configuration for the affected systems.

7.8 Configuration Verification & Audit

- Configuration verification and auditing increases software visibility and establishes traceability of changes throughout a CI, system or application lifecycle and confirms the configuration baseline has been fulfilled.

- Configuration verification and auditing is performed to ensure that configuration management processes are followed and that the integrity of the configuration baselines are maintained. Specifically, configuration audits ensure that:
  - System and application baselines are complete, correct and consistent to the established functional and physical specifications,
  - Approved changes were correctly implemented and verified, and
  - No unauthorized changes have occurred.

8.0 Roles and Responsibilities

8.1 Chief Information Officer (CIO) is responsible for:

- Approving and issuing policies, procedures, and guidance for implementing and managing the HUD Configuration Management Program.

- Ensuring the CM Program is integrated with the IT Capital Planning, PPM Life Cycle, and Technical Review Sub-Committee and CCMB governance processes.

- Directing, monitoring, and enforcing implementation and compliance with the HUD CM Program that includes CM planning, identifying and implementing configurations, controlling configuration changes, and monitoring.

- Designating a SecCM Program Manager for the organization and approving the organizational SecCM plan and policies.

8.2 Change Control Management Board (CCMB) is responsible for:

- Providing oversight and management of the HUD Secure Configuration Management Program.

- Developing secure configuration management policies and procedures and providing program direction and guidance.

- Establishing a secure and sound configuration management framework for defining, maintaining, and reviewing system and application baseline configuration documentation and the identification, management and tracking of associated hardware, software, and associated configuration items for each HUD system.

- Establishing a formal process for identifying, validating, and disposing of proposed changes to the HUD IT Infrastructure, systems, and applications products and configuration baselines throughout the system lifecycle. No hardware, software, service, interface, or other IT configuration item will be considered a Departmental standard or deployed until it has been approved by the CCMB.

- Conducting CCMB meetings to maintain a centralized process for reviewing, controlling, and monitoring all changes made to HUD's IT infrastructure, systems, and applications employed to meet HUD's business requirements.

- Ensure that all systems and applications baseline configurations and subsequent changes are evaluated for security and risk impacts, costs, and schedule requirements, tested for compliance to HUD policies and guidance, and proceed through the CCMB process before implementation.

- Creating a centralized CM documentation repository and ensuring that HUD Configuration and Change Management process documents are maintained as a configuration item component and placed under configuration management control, including documentation of approved IT standard hardware, software, services, and other IT configuration items.

- Establishing and monitoring CM performance metrics and providing reports on the effectiveness of the CM Program activities to OCIO and Program Office leadership.

- Providing CM guidance and training to effectively communicate requirements and address questions and concerns regarding the interpretation of this policy and accompanying procedure.

- Collaborating and consulting with HUD Program Offices (Headquarters and Regions) in the implementation of CM Programs and processes.

- Coordinating with IOO and other security-related programs to perform secure configuration checks of systems by leveraging scans from CDM, Security Operations Center (SOC), and other available security tools, as well as other resources such as service and help desk requests and change requests. If unapproved configurations are found, the CCMB will notify System Owners (SO), ISSOs, and ITPM and request an explanation and a POA&M to identify the steps to address the deviation.

- Actively monitoring and conducting auditing activities to confirm CM compliance.
- Results of CM monitoring are reported to the CCMB. When inconsistencies are discovered as a result of monitoring activities, the CCMB may take remedial actions, as appropriate.

- The CCMB will consolidate and analyze monitoring reports to generate metrics associated with the HUD 's CM program overall performance.

8.3 Chief Information Security Officer (CISO) is responsible for:

- Ensuring HUD's Secure Configuration Management (SecCM) requirements comply and align with federal configuration management guidance and Information Technology (IT) security policies and procedures.

- Providing staff with security expertise to serve on the CCMB and to conduct security impact analysis reviews, as necessary.

- Providing guidance on managing system configurations and defining controls that support establish and maintain secure system configurations, and support for managing security risks in systems and applications.

- Reviewing baseline configuration packages and continuously monitor the effectiveness of all controls selected, implemented, and authorized for protecting HUD information, systems, and applications.

- Establishing risk-based policy standards for federal information and information systems for cost-effective security and privacy and the Information Security Continuous Monitoring (ISCM) process to maintain an ongoing awareness of information security, vulnerabilities, and threats to support HUD risk management decision.

- Ensuring information security considerations for individual information systems, including the specific authorization decisions for those systems, are viewed from an organization-wide perspective about the overall strategic goals and objectives of the organization.

- Facilitating the sharing of security-related and risk-related information among Authorizing Officials (AO) and other senior leaders in the organization to help those officials consider all types of risks that could affect mission and business success and the overall interests of the organization at large.

- Ensuring System Owners (SO), ISSOs, and AOs monitor and manage system and application risks, as part of the overall configuration controls and risk management strategy.

8.4 Infrastructure and Operations Office (IOO) is responsible for:

- Providing operational procedures, standards, and guidance related to operational CM (OpsCM) for systems and applications in support of the HUD's Configuration Management Policy.

- Ensuring GSS system administrators comply with IT policies and procedures, implement agreed-upon secure baseline configurations, incorporates secure configuration settings for IT products, and assists with security impact analyses and configuration monitoring activities as needed.

- Working with GSS system administrators in the process for determining the appropriate baseline configuration for each configuration items and enforce compliance with secure configuration management policies and operational procedures.

- Instituting infrastructure change management processes that align with policy and the CCMB.

- Implementing and managing CDM tools to monitor HUD's enterprise infrastructure environment, detect and report on CM changes, and providing vulnerability monitoring.

- Providing basic enforcement of CM baseline configurations by requiring that all systems and applications submitted through the Technical Review Sub-Committee (TRC) and approved by the CCMB are implemented and controlled by the applicable SCM tool and procedures available within HUD's infrastructure.

- Reviewing system and application release requests to ensure compliance with the published policies, standards, and procedures and approving the release via the confirmation of testing and HARTS document that includes a CCMB-approved product and/or change request. Non-compliance with CM documentation requirements or failures due to qualify assurance (QA) issues during Stage testing will result in the rejection of the release request and notification to the ITPM, CCMB, and TRC. To mitigate and/or eliminate risks or disasters from reaching our production infrastructure, systems undergo unit, stress, and environmental testing in the Stage environment prior to release.

8.5 IT Program and Project Management Personnel (ITPMs) are responsible for:

- Assuring all systems and applications comply with the HUD IT policies and CCMB processes.

- Collaborating with System Owners to ensure adequate CM resources are available to monitor and address any changes to their information systems configurations and ensuring that

control settings are appropriately identified, tested, validated, approved, and subsequently documented within the appropriate system and configuration documentation (e.g. configuration management plans, system component inventories, technical specification and design documentation, system security documentation, etc.), the CCMB SharePoint site, and monitoring tools.

- Facilitating the development and documentation of the system or application baseline configuration during the development life cycle phase that is complete, accurate and presents minimal risk.

- Establishing and maintaining configuration change management control of assigned systems and applications based on a formal configuration management plan that adhere to change management policies and CCMB processes.

- In the event of incidents or other emergency requirements occur that would result in changes to a systems configuration, the IT PM will support the SO to obtain approval for system or application changes from the CCMB before release and implementation. After implementation, the system should be reactively assessed for security and risk impact to the HUD environment within 30 days after release.

- Baseline configurations reviews are conducted, at a minimum, annually by ITPM with support from the SO, ISSO, and the designated CM resources to assess the secure state of their system and confirm that all changes are accurately and completely documented in the configuration baseline documentation. Results of these self-assessments are submitted to the CCMB.

- Participating with the SO, ISSO, and other appropriate resources in configuration audit activities that focus on reviewing audit results and documenting the final disposition of configuration audits.

- Participating in configuration conflict resolution sessions, during the PPM execution and control phase, if configuration conflicts are found. The prioritization process will involve the IT Project Manager or Program Manager (ITPM), SO, HUD IOO resources, and the Risk Manager and Chief Information Security Officer (CISO), as needed.

- Working with the SO to analyze and resolve baseline configuration deviations identified through security and CDM scans and develop the required documentation to address issue and ensure that the baseline configuration information is correct, including POA&Ms and Request for Change forms.

8.6 System Owner (SO) is responsible for:

- Ensuring each of their systems and applications are planned, developed, deployed, and operated in compliance with established IT policies and procedures.

- Ensuring application system administrators comply with IT policies and procedures, adhere with secure baseline configurations, incorporates secure configuration settings for IT products, and assists with security impact analyses and configuration monitoring activities.

- Working with ISSO and ITPM to identify, define, implement, and maintain secure configurations for each application that have not been defined by the OCIO, and communicate all associated risks to AO for concurrence.

- Ensure all misconfigurations or related vulnerabilities discovered during security scans are reported to the ISSO and ITPM for mitigation.

- Implementing security and privacy controls to effectively protect their assigned information, data, and IT systems and applications and establishing baseline configurations that are secure and present minimum risk.

- Completing Security Assessment and Authorization (SA&A) and continuous monitoring activities.

- Maintaining and reporting POA&Ms to address vulnerabilities and risks in compliance with HUD policies and guidance.

- Ensuring an ISSO is designated in writing for each IT system and application under their purview.

- Ensuring adequate CM resources are identified and trained for planning, monitoring, and processing any changes to their information systems configurations and ensuring that control settings are appropriately identified, tested, validated, approved, and subsequently documented within the appropriate system and configuration documentation (e.g. configuration management plans, system component inventories, technical specification and design documentation, system security documentation, etc.) stored in the CCMB SharePoint site and CM monitoring tools.

- Ensuring that risk management activities include enforcing and tracking configuration and supply chain management plans and processes to control product evolution of all configuration items during the system and application operational life of all hardware and software, including supply chain activities required to repair, replace, or modify configuration items.

- Developing a full life cycle plan based on the established life expectancy of the product and total cost of ownership. Any new or existing product that will reach end-of-life (EOL) within three (3) years and is part of a component IT system will require the development of remediation, upgrade, replacement, and funding plan to prevent the EOL items and adhere to HUD standard products and associated versions. Any deviations from this policy requires that a plan of action and milestone be submitted for risk acceptance to the Authorizing Official (AO) and CISO to track remediation milestones appropriately.

- Coordinating with system owners of General Support Systems (GSS) that host their applications to confirm:

    - Fully implemented secure baseline configurations;

    - The adequacy of those GSS security controls to protect applications and identify and implement compensatory controls when risks are identified; and

    - All system and application components are maintained at the standard versions, tested as required, and all End-of-Life (EOL) or End-of Support (EOS) issued are circumvented.

- Ensuring adequate CM resources are available to monitor and be prepared to address any needed changes to their information systems configurations and settings are appropriately requested, tested, validated, approved, and subsequently documented within the appropriate system and configuration documentation (e.g. configuration management plans, system component inventories, technical specification and design documentation, system security documentation, etc.), the CCMB SharePoint site, and monitoring tools.

- In the event of incidents or other emergency services occur that would result in changes to a systems configuration, the IT PM and SO must receive sign off from leadership before release and implementation. After implementation, the system should be reactively assessed for security and risk impact to the HUD environment within 30 days after release.

- Collaborates with the HUD Test Center and Chief Information Security Officer (CISO) to perform risk assessments and technical testing and examination techniques[20] to identify and address all issues and vulnerabilities in a timely manner.

- Ensures system developer resources are building secure configuration settings into applications in accordance with security requirements and assists with security impact analyses and configuration monitoring activities as needed. In addition, the developer may be included in the process for determining the appropriate baseline configuration for relevant CIs and may serve on the CCB. Developers are also responsible for complying with SecCM policies and implementing and following secure configuration management procedures.

8.7 Information System Security Officer (ISSO) is responsible for:

- Working with the SO on the implementation of configuration management controls for each system and application.

- Working with the SO on evaluating proposed configuration changes and determining the impact of the change to the security of the system or application.

[20] NIST SP 800-115, Technical Guide to Information Security Testing and Assessment

- Conducting configuration monitoring activities (reporting and analysis).

- Working with the SO to document and assess all configuration deviation requests are within an agreed upon level of risk acceptance.

8.8 Authorizing Official (AO) is responsible for:

- Formally assuming responsibility for operating an information system that is implemented with a minimal level of risk.
- Ensuring CM resources are identified and documented within all IT Capital Planning, PPM, and Configuration Management activities, documents and templates to address configuration management compliance requirements throughout the life cycle of the investment, system, or application.
- Providing staff to manage systems and applications that comply with IT policies and procedures and identifying resources for security activities, determining the acceptability of system and application configuration controls and security assessment and authorization (SA&A) documentation, and determining risk to agency operations, agency assets, and individuals.

- Coordinating with the HUD Risk Executive on secure configuration management issues and making the final determination whether or not a given change or set of changes continues to be an acceptable security risk.

8.9 Technical Review Committee (TRC) is responsible for:

- Establishing and maintain the Secure CM Policy, which shall ensure that all changes are assessed, approved, implemented, and reviewed in a controlled, end-to-end manner.

- Providing oversight to both operational change requests and to project (PMBOK) change requests.

- Ensuring standardized methods and procedures are used for efficient and prompt handling of all changes to enterprise services and projects.

- Minimizing the impact of change-related incidents upon service quality, and consequently improve the day-to-day operations of the organization.

- Conducting change and configuration management assessments which may lead to changes in architectural and technical standards; however, these should be considered independent functions. Change requests not meeting established target architecture or technical standards shall be denied until the target architecture or technical standards are changed.

9.0 Definitions of Key Terms

Baseline Configuration - A documented set of specifications for a system, or a configuration item 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.

Common Secure configuration - A recognized standardized and established benchmark (e.g., National Checklist Program, DISA STIGs, CIS Benchmarks, etc.) that stipulates specific secure configuration settings for a given IT platform.

Configuration Item - An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process.

Configuration Settings - The set of parameters that can be changed in hardware, software, and/or firmware that affect the security posture and/or functionality of the information system.

Least functionality – To configure information systems to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, and/or services that are not integral to the operation of the system.

Misconfiguration - An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.

Secure Configuration Management - The management and control of configurations for an information system to enable security and facilitate the management of risk.

Security Content Automation Protocol (SCAP) - A protocol currently consisting of a suite of seven specifications that standardize the format and nomenclature by which security software communicates information about software flaws and security configurations.

Security Impact Analysis - The analysis conducted by an organizational official to determine the extent to which a change to the information system have affected the security state of the system.

System Component - A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.

Stack Requirements – Listing of all technology, services, frameworks, codes, languages, etc. to operate a product.

Traceability Matrix – A matrix that records the relationship between two or more products of the development process (e.g., a matrix that records the relationship between the requirements and the design of a given software component). Note 1: A traceability matrix can record the relationship between a set of requirements and one or more products of the development process and can be used to demonstrate completeness and coverage of an activity or analysis based upon the requirements contained in the matrix. Note 2: A traceability matrix may be conveyed as a set of matrices representing requirements at different levels of decomposition. Such a traceability matrix

enables the tracing of requirements stated in their most abstract form (e.g., statement of stakeholder requirements) through decomposition steps that result in the implementation that satisfies the requirements. The matrix should also include security requirements of the product(s).

Security Configuration Management - The management and control of configurations for an information system to enable security and facilitate the management of risk.

10.0 Related Documents and References

- National Institute of Standards and Technology (NIST) 800-128, Guide for Security-Focused Configuration Management of Information Systems
- NIST Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-47, Managing the Security of information Exchanges
- NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-160, Engineering Trustworthy Secure Systems
- NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- NIST Interagency Report 8011, Automation Support for Security Control Assessment:
    - Volumes 1: Overview
    - Volume 2: Hardware Asset Management
    - Volume 3: Software Asset Management

    - Volume 4: Software Vulnerability Management
- OMB M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices
- HUD IT Security Policy, HUD Handbook 2400.25
- HUD Policy for IT Project Planning and Management (PPM), HUD Handbook 3410.1
- HUD Project Planning and Management (PPM) Life Cycle V2.0
- Software Configuration Management (SCM) Policy, HUD Handbook 3252.1
- Change Management Policy, HUD Handbook 3253.1
- Enterprise Patch Management Policy, HUD Handbook 3254.1
- Software Configuration Management Procedures ver. 17, June 2020

Industry Consensus Common Secure Configuration Guidelines

- Center for Internet Security (CIS) Benchmarks https://www.cisecurity.org/cis-benchmarks/
- DoD Cyber Exchange Public Standard Technical Implementation Guidelines (STIG) https://public.cyber.mil/stigs/
- National Institute of Science and Technology (NIST) National Checklist Program https://nvd.nist.gov/ncp/repository
- United States Government Configuration Baselines (USGCB) https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline/USGCB-Content