



IT Security Handbook

Configuration Management

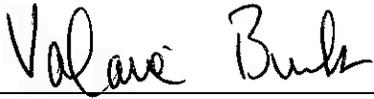
ITS-HBK-2810.07-01 -
Effective Date: 20110506 -
Expiration Date: 20130506 -
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

ITS Handbook (ITS-HBK-2810.07-01)
Configuration Management

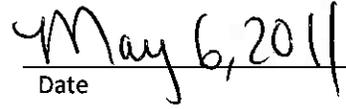
Distribution:

NODIS

Approved



Valarie Burks
Deputy Chief Information Officer for
Information Technology Security



Date

Change History

Version	Date	Change Description
1.0	5/2/11	Initial Draft

Table of Contents

Change History	3 -
1 Introduction and Background	5 -
2 Baseline Configuration (CM-2)	5 -
3 Configuration Change Control (CM-3)	6 -
4 Security Impact Analysis (CM-4)	6 -
5 Access Restrictions for Change (CM-5)	6 -
6 Configuration Settings (CM-6)	6 -
7 Least Functionality (CM-7)	7 -
8 Information System Component Inventory (CM-8)	7 -
9 Configuration Management Plan (CM-9)	7 -
10 Organizationally Defined Values	9 -

1 Introduction and Background

- 1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).
- 1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.
- 1.3 - NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.
- 1.4 - *NPR 2810.1, Security of Information Technology*, designates this handbook as a guide of NASA's Configuration Management (CM) information security controls.
- 1.5 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.
- 1.6 - The Configuration Management control family relates to the organizational aspects of information system baseline configurations, establishing review and validation, and change control. The control family also manages administrator roles, and the ability of individuals to make changes to the information systems' configuration. The concept of configuration management is critical to the continuous monitoring processes. Strict methodologies for the regulation of information system baselines and changes to system configurations are necessary for near real-time understanding of a system's risk posture.
- 1.7 - **Applicable Documents**
- *NPD 2810.1, NASA Information Security Policy*
 - *NPR 2810.1, Security of Information Technology*
 - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
 - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
 - *NIST SP 800-128, Guide for Security Configuration Management of Information Systems*

2 Baseline Configuration (CM-2)

- 2.1 - **Roles and Responsibilities**
- 2.1.1 *The Information System Owner (ISO) shall:*
- 2.1.1.1 - Establish and maintain a documented specification to which information systems are built as a part of the initial system development phase in a manner consistent with organizationally defined values.
 - 2.1.1.2 - Document any and all deviations from baseline configurations, as defined by the Agency Security Configuration Standards (ASCS) project.

3 Configuration Change Control (CM-3)

3.1 Roles and Responsibilities

3.1.1 *The ISO shall:*

- 3.1.1.1 - Ensure all configuration changes are documented in the system's security documentation (e.g., System Security Plan) through the NASA Security Assessment and Authorization Repository (NSAAR) in a manner consistent with organizationally defined values.

4 Security Impact Analysis (CM-4)

4.1 Roles and Responsibilities

4.1.1 *The ISO shall:*

- 4.1.1.1 - Ensure potential security impacts are analyzed prior to the implementation of information systems or changes to information systems, and if implemented, that impacts are documented in the system's security documentation (e.g., System Security Plan) through the NSAAR.

5 Access Restrictions for Change (CM-5)

5.1 Roles and Responsibilities

5.1.1 *The ISO shall:*

- 5.1.1.1 - Define and document logical and physical access restrictions to making changes to information systems in the system's security documentation (e.g., System Security Plan) through the NSAAR, in a manner consistent with organizationally defined values.
- 5.1.1.2 - Manage individuals' logical and physical access privileges to change information systems in a manner consistent with organizationally defined values.
- 5.1.1.3 - Ensure the capability to audit information systems in order to detect unauthorized changes in a manner consistent with organizationally defined values.

6 Configuration Settings (CM-6)

6.1 Roles and Responsibilities

6.1.1 *The Senior Agency Information Security Officer (SAISO) shall:*

- 6.1.1.1 - Ensure the creation of Agency-wide recommended configuration settings for commonly used devices (e.g., Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB), and Center for Internet Security (CIS) baselines).

6.1.2 *The Center Chief Information Security Officer (CISO) shall:*

- 6.1.2.1 - Review and approve systems that cannot be equipped with Agency-defined configuration status monitoring, and patch management and reporting tools.
- 6.1.2.2 - Coordinate with ISOs to determine if detected changes to configuration settings are the result of an incident to be reported to the Security Operations Center (SOC).

6.1.3 *The Organization Computer Security Official (OCSO) shall:*

- 6.1.3.1 - Review and approve systems that cannot be equipped with Agency-defined configuration status monitoring, and patch management and reporting tools.
- 6.1.3.2 - Coordinate with ISOs to determine if detected changed to configuration settings are the result of an incident to be reported to the SOC.

6.1.4 *The ISO shall:*

- 6.1.4.1 - Ensure that information systems are equipped with Agency-defined configuration status monitoring, and patch management and reporting tools.

Configuration Management -

- 6.1.4.2 - Seek approval from the Center CISO or OCSO for systems that are cannot be equipped with Agency-defined - configuration status monitoring, and patch management and reporting tools. -
- 6.1.4.3 - Determine, in collaboration with the Center CISO or OCSO, if detected changes in configuration settings are the - result of an incident to be reported to the SOC. -
- 6.1.5 *The ASCS Project Manager shall:* -
 - 6.1.5.1 - Provide assessments, recommendations, processes, procedures, and reports for system configuration - requirements in compliance with federal mandates and recommendations. -
- 6.1.6 *The Agency Security Update System (ASUS) Project Manager shall:* -
 - 6.1.6.1 - Ensure the capability to monitor and report on the configuration and patch status of information systems across - the Agency. -
- 6.1.7 *The SOC shall:* -
 - 6.1.7.1 - Ensure detected events regarding unauthorized security-relevant configuration changes are documented as - security incidents in the NASA Incident Management System (IMS). -

7 Least Functionality (CM-7)

- 7.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security - categorization and risk environment of the information and/or information system. -

8 Information System Component Inventory (CM-8)

8.1 - Roles and Responsibilities

- 8.1.1 *The Information Technology Security Enterprise Data Warehouse (ITSec-EDW) Project Manager shall:* -
 - 8.1.1.1 - Ensure the capability to inventory all Agency information system component devices and networks. -
 - 8.1.1.2 - Ensure the capability to associate all information system component devices and networks with a System Security - Plan (SSP). -
 - 8.1.1.3 - Ensure the capability to automatically collect and correlate patch statistics, vulnerability scan results, hardware - and software data, security configurations, and information from other data sources. -
 - 8.1.1.4 - Ensure the capability to automatically detect devices which are newly connected to NASA networks. -
 - 8.1.1.4.1 - Tools and/or data to regarding newly connected devices should be provided to Center CISOs, OCSOs, and ISOs as - appropriate. -
 - 8.1.1.5 - Ensure the capability to disable network access to those devices which are identified as unauthorized. -
- 8.1.2 *The ISO shall:* -
 - 8.1.2.1 - Ensure that all information system component devices and networks are documented in ITSec-EDW and associated - with a SSP. -

9 Configuration Management Plan (CM-9)

9.1 - Roles and Responsibilities

- 9.1.1 *The ISO shall:* -
 - 9.1.1.1 - Implement and document, through NSAAR, a Configuration Management Plan which includes the following: -
 - 9.1.1.1.1 - Roles, responsibilities, and processes and procedures for configuration management of information systems; -
 - 9.1.1.1.2 - Configuration items for information systems and when in the development life cycle the configuration items are - placed under configuration management; -
 - 9.1.1.1.3 - A means for identifying configuration items and the processes for those items' control and management; -
 - 9.1.1.1.4 - Key management stakeholders responsible for reviewing and approving proposed changes to information systems; - and -

- 9.1.1.1.5 Personnel responsible for conducting security impact analysis of information systems and changes to those systems.

10 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
CM	01	Configuration Management Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
CM	02	Baseline Configuration	E 1	[1]	Frequency	Baseline configuration reviews and updates.		1/Year	1/Year
CM	02	Baseline Configuration	E 1	[2]	Reference	Baseline configuration out-of-cycle review circumstances.		Significant change to system component.	Significant change to system component.
CM	02	Baseline Configuration	E 4	[1]	Reference	List of unauthorized software.			
CM	02	Baseline Configuration	E 5	[1]	Reference	List of authorized software.			
CM	03	Configuration Change Control	Main	[1]	Reference	Change control element.		Configuration Control Board (CCB)	Configuration Control Board (CCB)
CM	03	Configuration Change Control	Main	[2]	Selection	Change control element convene triggers.		Regular and Conditional	Regular and Conditional
CM	03	Configuration Change Control	Main	[2] [1]	Frequency	Change control element convene trigger.		4/Year	4/Year
CM	03	Configuration Change Control	Main	[2] [2]	Reference	Change control element convene trigger.		Significant change to system component.	Significant change to system component.

ITS Handbook (ITS-HBK-2810.07-01) -
Configuration Management -

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
CM	03	Configuration Change Control	E 1	[1]	Time Period	Duration until highlighted for lack of approval.			15 Days
CM	03	Configuration Change Control	E 4	[1]	Reference	Change control element.		Configuration Control Board (CCB)	Configuration Control Board (CCB)
CM	05	Access Restrictions for Change	E 2	[1]	Frequency	Audits of system changes.			4/Year
CM	05	Access Restrictions for Change	E 3	[1]	Reference	Critical software prevented from installation without signed certificates.			Device Drivers; ISO-Defined Software
CM	05	Access Restrictions for Change	E 4	[1]	Reference	Information system components enforcing two-person rule for changes.			
CM	05	Access Restrictions for Change	E 5	[1]	Frequency	Review of developer/integrator privileges.			
CM	05	Access Restrictions for Change	E 7	[1]	Reference	Automated means for safeguarding inappropriate security function changes.			
CM	06	Configuration Settings	Main	[1]	Reference	Mandatory configuration settings.	FDCC, USGCB, or CIS Benchmarks	FDCC, USGCB, or CIS Benchmarks	FDCC, USGCB, or CIS Benchmarks
CM	06	Configuration Settings	E 2	[1]	Reference	Configuration settings with automated responses to unauthorized changes.			Any System Administrator-Level Changes
CM	07	Least Functionality	Main	[1]	Reference	List of prohibited or restricted functions, ports, protocols, and/or services.	ISO-Defined	ISO-Defined	ISO-Defined
CM	07	Least Functionality	E 1	[1]	Frequency	Review of information system for identification of unnecessary functions, ports, protocols, and/or services.		4/Year	4/Year

ITS Handbook (ITS-HBK-2810.07-01) -
Configuration Management -

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
CM	07	Least Functionality	E 2	[1]	Selection	Program execution is automatically managed in accordance with.			ISO-Defined Unauthorized Software
CM	07	Least Functionality	E 3	[1]	Reference	Registration requirements for ports, protocols, and services.			
CM	08	Information System Component Inventory	Main	[1]	Reference	Information necessary for managing accountability in inventories of information system components.	Vendor/Manufacturer Name and Component Name	Vendor/Manufacturer Name and Component Name	Vendor/Manufacturer Name and Component Name
CM	08	Information System Component Inventory	E 3	[1]	Frequency	Check for unauthorized components/devices added to the system.			1/Day
CM	08	Information System Component Inventory	E 4	[1]	Selection	Identification criteria for individuals responsible for administering information system components.			Position or Role