For High-Impact Information Systems

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

CM-1.1 – **Examine** configuration management policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with configuration management and control responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents configuration management policy and procedures;				
(ii)	The organization disseminates configuration management policy and procedures to appropriate elements within the organization;				
(iii)	Responsible parties within the organization periodically review configuration management policy and procedures; and				
(iv)	The organization updates configuration management policy and procedures when organizational review indicates updates are required.				

CM-1.2 - Examine configuration management policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with configuration management and control responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The configuration management policy addresses purpose, scope, roles and responsibilities, management commitment, coordination				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	among organizational entities, and compliance;				
(ii)	The configuration management policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and				
(iii)	The configuration management procedures address all areas identified in the configuration management policy and address achieving policy-compliant implementations of all associated security controls.				

CM-2 BASELINE CONFIGURATION - The organization develops, documents, and maintains a current baseline configuration of the information system.

CM-2.1 – Examine configuration management policy; procedures addressing the baseline configuration of the information system; Federal Enterprise Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & ate
(i)	The organization develops, documents, and maintains a baseline configuration of the information system;				
(ii)	The baseline configuration shows relationships among information system components and is consistent with the Federal Enterprise Architecture;				
(iii)	The baseline configuration provides the organization with a well-defined and documented specification to which the information system is built; and				
(iv)	The organization documents deviations from the baseline configuration, in support of mission needs/objectives.				

CM-2(1).1 – Examine configuration management policy; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & ate
(i)	The organization identifies the frequency of updates to the baseline configuration and instances that trigger configuration updates; and				
(ii)	The organization updates the baseline configuration of the information system as an integral part of information system component installations.				

CM-3 CONFIGURATION CHANGE CONTROL - The organization authorizes, documents, and controls changes to the information system.

CM-3.1- Examine configuration management policy; procedures addressing information system configuration change control; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization authorizes, documents, and controls changes to the information system;				
(ii)	The organization manages configuration changes to the information system using an organizationally approved process; and				
(iii)	The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws.				

CM-4 MONITORING CONFIGURATION CHANGES - The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.

CM-4.1 – Examine configuration management policy; procedures addressing the monitoring of configuration changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies the types of information system changes to be monitored;				
(ii)	The organization monitors changes to the information system; and				
(iii)	The organization conducts security impact analyses to assess the effects of the information system changes.				

CM-5 ACCESS RESTRICTIONS FOR CHANGE - The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.

CM-5.1 – Examine configuration management policy; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization maintains a list of qualified and authorized personnel permitted to access the information system for the express purpose of initiating changes;				
(ii)	The organization approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and				
(iii)	The organization generates, retains, and reviews records reflecting all such changes to the information system.				

and

Test Change control process and associated restrictions for changes to the information system.

Test Steps	S	N	Findings	Initials & Date

	Test Steps	S	N	Findings	Initials & Date
1					

CM-6 CONFIGURATION SETTINGS - The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.

CM-6.1 - Examine configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST Special Publication 800-70; other relevant documents or records to determine if the following requirements are met:

	Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization establishes mandatory configuration settings for information technology products employed within the information system;				
(ii)	The organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements;				
(iii)	The organization documents the configuration settings; and				
(iv)	The organization enforces the configuration settings in all components of the information system.				

and

Test information system configuration settings to determine if the following requirements are met:

	Test Steps	S	N	Findings	Initials & Date

Test Steps		S	N	Findings	Initials & Date
1	Validate that the system configurations settings coincide to the organization's documented settings.				

CM-7 LEAST FUNCTIONALITY - The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services].

CM-7.1 - Examine configuration management policy; procedures addressing least functionality in the information system; information system security plan (for list of organization-defined prohibited or restricted functions, ports, protocols, and services for the information system); information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies prohibited or restricted functions, ports, protocols, and services for the information system;				
(ii)	The organization configures the information system to provide only essential capabilities; and				
(iii)	The organization configures the information system to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.				

and

Test information system configuration settings to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Validate that the system configuration settings comply with the organizationally-defined settings for least functionality through restricted privileges, ports, protocols and/or services.				

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY - The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.

CM-8.1 - Examine configuration management policy; procedures addressing information system component inventory; information system inventory records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops, documents, and maintains a current inventory of the components of the information system; and				
(ii)	The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability.				

CM-8(1).1 - Examine configuration management policy; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records, **and**

Interview organizational personnel with information system installation and inventory responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization updates the inventory of information system components as an integral part of component installations.				