



COMDTINST 5230.69
OCT 26 2004

COMMANDANT INSTRUCTION 5230.69

Subj: COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS AND INFORMATION TECHNOLOGY (C4&IT) CONFIGURATION MANAGEMENT (CM) POLICY

Ref: (a) Establishment of the CG-6 Directorate and Associated Duties, COMDTINST 5401.5 (series)

1. PURPOSE. This Instruction establishes the authority, roles, and responsibilities governing Configuration Management (CM) for Command, Control, Communications, Computers and Information Technology (C4&IT) systems. CM is a process for establishing and maintaining consistency of an asset's performance, functional, logical, and physical attributes with its requirements, design, and operational information throughout its life cycle. CM ensures the availability and proper functioning of an asset or system as a result of a change to the asset or system. This policy applies to all C4&IT assets, including systems and products that enable C4&IT capability in support of the Coast Guard's missions or business functions. All Coast Guard organizations involved in the planning, acquisition, production, deployment, support, operations, and disposition of C4&IT assets shall employ the C4&IT CM policy and adhere to the roles defined herein.
2. ACTION. Area and District commanders, commanders of maintenance and logistics commands, commanding officers of Headquarters units, assistant commandants for directorates, Chief Counsel, and special staff offices at Headquarters shall ensure that all Coast Guard and contractor support personnel or organizations involved in the acquisition, development, operations, maintenance or use of Coast Guard C4&IT systems comply with the provisions of this Instruction. Internet release is authorized.
3. DIRECTIVES AFFECTED. None.
4. CONFIGURATION MANAGEMENT (CM). CM is a process for establishing and maintaining consistency of an asset's performance, functional, logical, and physical attributes with its requirements, design, and operational information throughout its life cycle. The goal of CM and CG-6 is to guarantee availability and proper functioning of an asset and continued Integrated Logistics Support (ILS) as a result of a change to the asset. Elements of CM include:

DISTRIBUTION – SDL No. 141

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	1	1	1	1	1	1																				
B		8	10		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
C	1	1	1	1	1	1	1				2	1	1	2			1								1	
D	1	1		1	1															1						
E															1								1			
F																										
G																										
H																										

NON-STANDARD DISTRIBUTION:

- a. Configuration (Life Cycle) Management and Planning. This element consists of CM planning information and the resulting documented CM processes that determine the extent of allocation of the CM functional activities to CM practitioners.
 - b. Configuration Identification. This element includes the rigorous identification and documentation of physical and functional characteristics, identification of configuration items, and establishment of configuration baselines.
 - c. Configuration Change Control. Configuration change control provides strong enforcement of organization and version control.
 - d. Configuration Status Accounting. The CM activity concerning capture, storage, and access to configuration information needed to effectively manage assets and asset information.
 - e. Configuration Verification and Audit. The CM activities that verify a product and document set in order to create a Product Baseline.
 - f. Integrated Logistics Support (ILS). ILS refers to the discipline of planning, implementing, and sustaining logistics and support practices that ensure the operational availability of mission and business critical assets at minimal total ownership cost. ILS is a generic term that encompasses all support activities associated with developing, acquiring, testing, and sustaining the mission effectiveness of operating systems throughout their service lives.
5. CONFIGURATION MANAGEMENT ROLES AND RESPONSIBILITIES. The Commandant (CG-6) organization works proactively with all entities involved in the system life cycle. Figure 1: CG-6 Roles and Relationships Framework, as outlined in reference (a), illustrates the key roles involved and their relationships. The remainder of this section describes the roles, relationships, and responsibilities as they relate to this policy.
- a. CG-6. Chief Information Officer (CIO). The CIO is responsible for implementation of C4&IT CM throughout the Coast Guard. Specifically, CG-6 has the following responsibilities:
 - (1) Maintaining and approving the C4&IT CM policy and practice. To this end, CG-6 shall establish the C4&IT CM Policy Review Board to develop and maintain enterprise C4&IT CM policy aligned with Coast Guard policy.
 - (2) Authorizing establishment of C4&IT Configuration Control Boards (CCBs), as necessary, and publishing the list of authorized C4&IT CCBs.
 - (3) Delegating the execution of the CM practices to the roles defined herein.
 - b. Enterprise Steward. CG-6 provides enterprise-level stewardship of the policies and practices associated with the CM of C4&IT systems. The Enterprise Steward monitors the health, effectiveness, and efficiency of C4&IT CM and ensures organizational compliance.

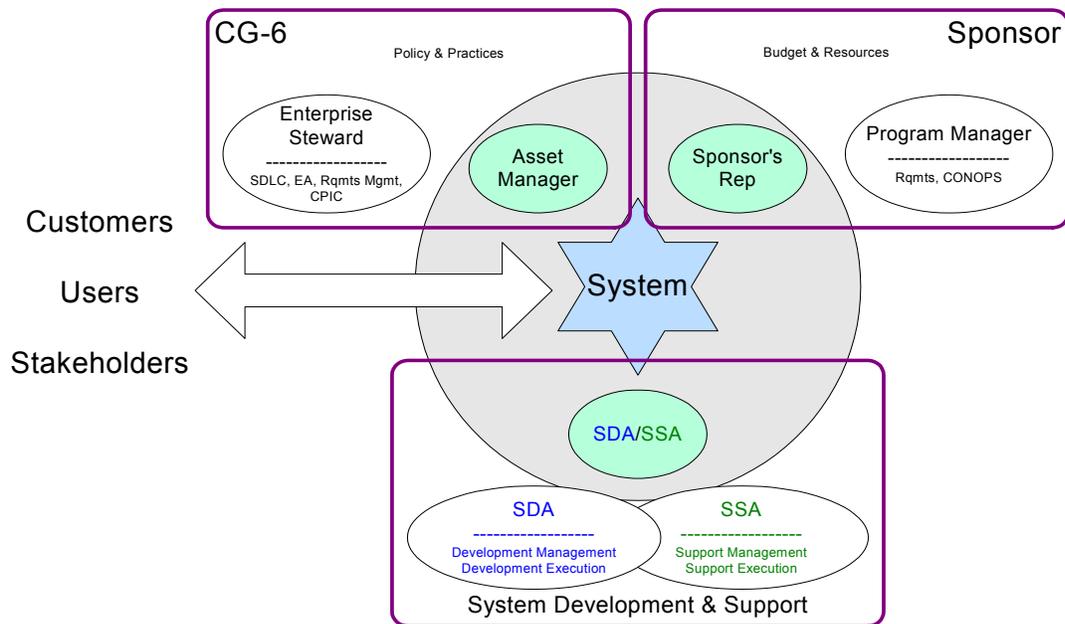


Figure 1: CG-6 Roles and Relationships Framework

- c. **Asset Manager.** The Asset Manager is designated by CG-6 to guide, oversee, and monitor CM policies and practices for the assigned system. An asset is a system, product (e.g., Commercial-off-the-Shelf equipment, information, policy), data, service, capability, or resource that is available, managed, delivered, applied, supported, or sustained on an enterprise scale by the CG-6 organization in collaboration with its supporting Program Sponsor and Manager, customers, and external stakeholders, System Development Agent (SDA), and System Support Agent (SSA). The Asset Manager has the following responsibilities:
- (1) Collaborating with the Program Manager or the Sponsor's Representative to facilitate alignment and compliance with Coast Guard CM policies and practices.
 - (2) Developing and recommending changes to CM policies and practices, as necessary, to enhance the quality of C4&IT systems and CM practices.
 - (3) Ensuring that CM performance measures are developed, tracked, and evaluated.
- d. **Sponsor.** The Sponsor is the organizational element that accepts C4&IT capability needed to support a Coast Guard mission or business function. The Sponsor is also responsible for:
- (1) Defining, maintaining, and articulating organization and program goals.
 - (2) Validating requirements developed by the Program Manager.
- e. **Program Manager.** The Coast Guard Program Manager is the Sponsor's designated manager who is responsible for:
- (1) Defining, maintaining, evaluating, and articulating program requirements.
 - (2) Advocating the end user's concerns and establishing or maintaining mechanisms that ensure that program requirements are being addressed through CM.
 - (3) Ensuring that CM training is defined, resourced, and provided and that CM performance measures are defined, tracked, and evaluated.

- (4) Coordinating, assimilating, and providing end user input to CM policies and practices.
- f. Sponsor's Representative. The Sponsor's Representative is designated by the Sponsor to serve as the liaison and interface for the Sponsor and the Sponsor's Program Manager to the other key roles involved in the CM of an asset. The Sponsor's Representative has the following CM responsibilities:
 - (1) Initiating change requests.
 - (2) Maintaining liaison with the appropriate CCBs, Asset Manager, technical staffs of the SDA and SSA, and the Sponsor.
 - (3) Representing all of the Sponsor's needs.
 - (4) Collaborating with the Program Manager or the Sponsor to facilitate alignment and compliance with Coast Guard CM policies and practices.
 - (5) Developing and recommending changes to CM policies and practices, as necessary, to enhance the quality of C4&IT systems and CM practices.
 - (6) Communicating with end users to gather input and feedback and to relay results regarding CM policies and practices.
- g. System Development Agent (SDA). The SDA is the individual, unit, firm, agency, or organization that performs, or has the responsibility for, the design, development, implementation, and support of C4&IT systems, as well as the acquisition of C4&IT products or services. The SDA has a critical role in the CM process. The SDA performs CM for assigned systems and is a technical advisor to the other stakeholders involved in CM, particularly the CCB. More than one SDA may be technical agents for the CCB. The SDA has the following responsibilities:
 - (1) Performing approved CM practices for assigned systems.
 - (2) Providing competent technical authority for the change being requested.
 - (3) Developing and submitting technical proposals to implement the requested change.
 - (4) Serving as technical evaluator for development issues and advisor to the CCB and other CM stakeholders.
 - (5) Collaborating with the Sponsor's Representative and the Asset Manager to define design and development requirements or solutions.
 - (6) Making design and development changes as approved by the CCB.
 - (7) Defining, tracking, and evaluating CM performance measures pertaining to development throughout the life cycle.
- h. System Support Agent (SSA). The SSA is the individual, unit, firm, agency, or organization that performs, or has the responsibility for, the maintenance, support, and availability of C4&IT systems. The SSA participates in all aspects of the CM process. The SSA has the following responsibilities:
 - (1) Performing approved CM practices for assigned systems.
 - (2) Serving the CCB and other CM stakeholders as the technical evaluator for support issues.
 - (3) Providing competent technical authority for the change being requested.

- (4) Providing competent technical authority for identifying, developing, and resolving support requirements associated with the change.
 - (5) Collaborating with the Sponsor's Representative and the Asset Manager to define support requirements and support solutions.
 - (6) Defining, tracking, and evaluating CM performance measures pertaining to support throughout the life cycle.
- i. User. The individual, unit, or organization that interacts with and uses C4&IT systems and services to accomplish work, execute missions, or deliver products and services to Coast Guard members and external customers. The user provides feedback on C4&IT systems and services, suggests enhancements to existing C4&IT systems or services, and identifies new system or service requirements via the Sponsor's Representative.
 - j. Customer. Any person or organization that benefits from C4&IT systems or services. An internal customer is a person or organization inside the Coast Guard for which the C4&IT system or service is being provided. An external customer is a person or organization outside the Coast Guard for which the C4&IT product or service is being provided. The customer suggests enhancements to existing C4&IT systems or services and identifies new system or service requirements via the Sponsor's Representative.
 - k. Stakeholder. Any person, group, or organization (e.g., customers, employees, suppliers, owners, Office of Management and Budget, Department of Homeland Security, or other agencies Congress) that can place a claim on, or influence, a C4&IT asset, is affected by that asset, or has a vested interest in, or expectation for, the asset. The stakeholder suggests enhancements to existing C4&IT systems or services and identifies new system or service requirements via the Sponsor's Representative.
 - l. C4&IT CCBs. These CCBs shall develop and maintain CM practices for their areas of responsibility. These practices must align and comply with the C4&IT Configuration and Management policy. The C4&IT CCBs may charter subordinate or Local Configuration Control Boards, as needed, if so authorized by their charter, for specific systems.
6. IMPLEMENTATION. CM practices establish the actions necessary to implement CM for all C4&IT assets. All Coast Guard organizations involved in the planning, deployment, support, operation, and disposition of C4&IT systems shall follow the C4&IT CM practice. CG-6 has final approval authority for these practices. CG-6 charters and delegates the primary development, maintenance, and review responsibility for these practices to the C4&IT CM Policy Review Board. The practices provide the procedures and processes for the following:
- a. C4&IT Enterprise CM. Provides the enterprise considerations for maintaining an effective CM program for C4&IT assets.
 - b. CCB Management. Serves as a governance structure for the establishment and management of CCBs.

7. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this Instruction and have been determined to be not applicable.
8. FORMS/REPORTS. None.

R.T. HEWITT /s/
Assistant Commandant for Command, Control,
Communications, Computers and
Information Technology (Acting)