



Commandant
U.S. Coast Guard

2100 2nd ST SW STOP 7901
Washington DC 20593-7901
Staff Symbol: CG-444
Phone: 202 475-5645

COMDTINST 4130.6A
MAY 24 2010

COMMANDANT INSTRUCTION 4130.6A

Subj: COAST GUARD CONFIGURATION MANAGEMENT POLICY

- Ref:
- (a) Information Management and Lifecycle Management Manual, COMDTINST M5212.12 (series)
 - (b) National Consensus Standard for Configuration Management, EIA-649 (series)
 - (c) Implementation Guide for Configuration Management, GEIA-HB-649 (series)
 - (d) Military Handbook Configuration Management Guidance, MIL-HDBK-61 (series)
 - (e) Software Life Cycle Processes, ISO 12207 (series)
 - (f) Major Systems Acquisition Manual (MSAM), COMDTINST M5000.10 (series)
 - (g) Non-Major Acquisition Process (NMAP), COMDTINST 5000.11 (series)
 - (h) Command, Control, Communications, Computers And Information Technology (C4&IT) Systems Development Life Cycle (SDLC) Policy, COMDTINST 5230.66 (series)
 - (i) DHS Acquisition Instruction/Guidebook 102-01-001 (series)
 - (j) Federal Acquisition Regulations System, Code of Federal Regulations-Title 48, Part 11.102
 - (k) Naval Engineering Manual (NEM), COMDTINST M9000.6 (series)
 - (l) Aeronautical Engineering Maintenance Management Manual, COMDTINST M13020.1 (series)
 - (m) Civil Engineering Manual, COMDTINST M11000.11 (series)

1. PURPOSE. The purpose of this Instruction is to restate and clarify Coast Guard (CG) policy on Configuration Management (CM) and change control.
2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements shall comply with the provisions of this Instruction. Internet release is authorized.

DISTRIBUTION – SDL No. 155

	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																		
B																										
C				1						1																
D																										
E		1					1																			
F																										
G																										
H																										

NON-STANDARD DISTRIBUTION:

3. DIRECTIVES AFFECTED. The following directives are hereby cancelled:
 - a. Coast Guard Configuration Management, COMDTINST 4130.6
 - b. Coast Guard Configuration Management for Acquisitions and Major Modifications, COMDTINST M4130.8
 - c. Coast Guard Configuration Management During Sustainment, COMDTINST M4130.9
 - d. Coast Guard Configuration Control Boards, COMDTINST M4130.10

4. BACKGROUND. The fundamental purpose of CM is to ensure that assets meet their requirements. An asset (or product) is something that is used or produced to satisfy a need, or is the result of a process. There are certain assets and administrative types of information that the CG must have to fulfill its mission, or that specifically impact safety, security, performance, schedule, cost, or the environment. For these critical assets, the CG must have a complete understanding of the performance, functional, and physical attributes of the asset, and how those attributes tie back to mission requirements. This configuration information is paramount to making timely and effective decisions regarding mission execution, mission support, and financial stewardship, and it is therefore imperative that consistency be maintained between these critical assets, their documented configuration, and the driving requirements. CG CM Policy is intended to support CG members in achieving that imperative.
 - a. This restatement of CG CM Policy does not so much represent a change in what is required of CG members as it does a change in how CG members must conduct CM-related activities, as well as emphasis of how important those activities are to the overall success of the CG. CG CM policy was originally designed to support a decentralized program that had both regional and area characteristics. While effective to some level, numerous studies and initiatives documented its shortcomings, and audit agencies have produced repeated Notices of Findings and Recommendation that identified a lack of standardized CM across the CG as an issue in conforming to financial, security, and safety regulations. This policy update requires a more centralized approach to CM, with standard processes that are effective between communities and across the lifecycle of critical assets, and provides that critical assets be viewed from a systems perspective, documentation about those assets be accurate and transparent, and changes to that documentation be accommodated and reflected in the asset in a timely fashion.
 - b. The fundamental purpose of the CG CM Policy is to meet requirements and accommodate change in a fiscally responsible way.

5. POLICY. It is CG policy to maintain rigorous CM over all critical assets and critical administrative information including but not limited to boats, aircraft, cutters, C4IT systems, people (billet structures, certification requirements and documentation), plans, business processes, financial processes, information systems, hardware, software, data, platforms, facilities, equipment, Navy Type Navy Owned (NTNO) products, and all contracted CM services (including performance based logistics support). CM shall be performed by documenting requirements; maintaining consistency between critical assets and their respective critical administrative information and approved configurations; and ensuring that approved changes to configurations are reflected in the configuration documentation. Official records created and/or received as documentation will be maintained and disposed of in accordance with reference (a). No member of the CG may change the configuration of critical assets or products or critical administrative information that is owned by the CG or owned by another agency, unless the change has been approved by the cognizant

Configuration Control Board (CCB) and documented in the configuration baseline. The prohibition on changing the configuration of critical assets or products or critical administrative information owned by the CG or other agencies without the approval of the cognizant CCB constitutes a general order, which is punitive in nature. Failure to comply with this order may result in disciplinary action under Article 92 of the Uniform Code of Military Justice for military members. Failure to comply with this order by civilian employees may result in disciplinary action in accordance with Civilian Personnel Actions: Discipline, Performance, Adverse Actions, Appeals, and Grievances, COMDTINST M12750.4 (series). See enclosure (1) for specific roles and responsibilities.

- a. CM Standards. The CG shall implement CM in accordance with reference (b) EIA-649A 2004 National Consensus Standard for Configuration Management with guidance from references (c), (d) and (e). See enclosure (2) for a list of the EIA-649 principles and enclosure (3) for key definitions of CM terms as they relate to the CG. References (a) through (j) are available at the CG Configuration Management site on the CG Portal.
 - b. Baselines. Configuration of critical CG assets shall be documented in configuration status accounting tools at levels necessary to design, construct, operate, support and dispose of an asset. The level of detail documented shall be tailored and proportionate to the product's scope, importance, complexity, production quantity, performance requirements, budget, and schedule. At a minimum, the configuration baseline shall identify the product's performance, functional, and physical attributes, including internal and external interfaces. The baseline shall also include traceability of the lowest level configuration items (CIs) to the highest level requirements (i.e., a traceability matrix). Authorized deviations from an asset's configuration baseline shall be documented.
 - c. Change Control Authority. Authority for changes to configuration baselines shall reside with cognizant CCBs. No changes shall be made to any asset under configuration control or to any configuration baseline without the approval of the cognizant CCB.
 - d. Lifecycle Management. All CG critical assets shall be acquired, designed, constructed, operated, sustained, and disposed of in accordance with references (a), (f), (g), (h) and (i) and the approved configuration baselines.
 - e. Standardization. The establishment of a configuration baseline for an asset shall satisfy the requirement for a standardization document in accordance with reference (j). All procurements, contracts, and acquisitions related to critical assets shall ensure that the configuration of the asset is maintained according to its approved configuration baseline.
6. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this Instruction and have been determined to be not applicable.

7. FORMS/REPORTS. None

D. PEKOSKE /s/
Vice Admiral, U.S. Coast Guard
Acting Commandant

- Encl: (1) Roles and Responsibilities
(2) Configuration Management Principles
(3) Key Definitions

ROLES AND RESPONSIBILITIES

1. Commandant (CG-444) is the Technical Authority representative for CG CM and shall:
 - a. Develop, implement and maintain CM policy.
 - b. Provide guidance and standards for CM implementation.
 - c. Define and evaluate enterprise level CM metrics.
 - d. Evaluate CM processes and report to Chief of Staff (future Deputy Commandant for Mission Support (DCMS)) on compliance with CM policies and process guides (i.e., instructions on how to perform a process).
 - e. Develop functional requirements for enterprise CM IT tools.
 - f. Provide guidance for CM professional development.
 - g. Act as the CG point of contact for interdepartmental (DHS/DOD) CM process issues.
 - h. Verify that all CM Plans (CMPs) and CCB charters are in accordance with standard CM process guides and CG CM policy
 - i. Verify that CM process guides meet CG CM policy requirements and resolve conflicts between process guides and other CG policies.
 - j. Review root cause closed loop corrective actions to facilitate compliance with CG CM policy and CM guidelines.
 - k. Identify and promote CM best practices to enable conformance to CM policy requirements
2. Executive Management Council is the executive-level CCB for all CG critical assets and shall charter subordinate CCBs as appropriate to delegate change control authority to the lowest level in the organization where change management can be effectively carried out.
3. Mission Support Directorates (CG-1, CG-4, CG-6, CG-9, DCMS-34, DCMS-5, and DCMS-8) shall:
 - a. Develop, implement and maintain CM plans such that the execution of CM processes within the directorate and by all vendors, suppliers and subcontractors conforms to the CG CM policy.
 - b. Develop, implement and maintain a plan to transition each product through its lifecycle phases.
 - c. Develop and implement CM process guides (i.e., instructions on how to perform processes) that conform to CG CM policy. The process guides should address identification of configuration items (CIs); configuration change management; and configuration audit and verification.
 - d. Update and maintain the Engineering Manuals in references (k), (l), and (m) such that they are consistent with the CM process guides.
 - e. Develop and maintain CM documentation for all critical assets, products and critical administrative information owned by the CG.

- f. Develop and implement CM audit and verification plans and root cause closed loop corrective actions that ensure compliance with CM policy and process guides within the directorate and by all vendors, suppliers and subcontractors. The CM audit verification and corrective action plans shall maintain or improve the accuracy of configuration data.
 - g. Establish internal CM audit and verification teams and define qualifications for their members.
 - h. Ensure that the identification and determination of CIs are based on the complexity, size, quantity, intended use and mission criticality as required to design, construct, operate, support and dispose of the product.
 - i. Ensure that Functional Configuration Audits (FCA) and Physical Configuration Audits (PCA) are completed and that all audit issues are resolved with root cause closed loop corrective actions prior to acceptance.
 - j. Throughout the lifecycle periodically verify that approved baselines have not been modified without authorization.
 - k. Provide Subject Matter Experts (SMEs) to evaluate proposed configuration changes.
 - l. Establish CCBs and specify the systems, CIs and baseline documentation for which each CCB has controlling authority.
 - m. Designate Configuration Managers and CCB chairs in writing and report the names to Commandant (CG-444).
 - n. Ensure that CM performance measures are tracked, evaluated and root cause closed loop corrective action plans are implemented for each product.
 - o. Develop execution plans to implement approved configuration changes.
 - p. Report summary results of all CM audits to the Chief of Staff (future DCMS). Reports shall include costs of implementing and restoring unauthorized changes as well as root cause closed loop corrective action plans.
 - q. Audit CM data for accuracy.
 - r. Ensure that Configuration Managers are trained in standard CM processes.
4. Commanders, Commanding Officers (CO) and Officers in Charge shall:
- a. Report product deficiencies and desired improvements to the acquisition and sustainment agents in accordance with designated process guides with copies to the Chief of Staff (future DCMS), Force Readiness Command (FORCECOM) and Area Commanders (future Operations Command (OPCOM)) via chain of command.
 - b. Only implement configuration changes that are approved by a CCB.
 - c. Make no unauthorized configuration changes to their assigned products.
 - d. Notify appropriate Logistics and Service Centers and the unit's Administrative Control (ADCON) for action regarding any unauthorized configuration changes or failure to achieve performance requirements. Provide same notification for information to the Chief of Staff (future DCMS), FORCECOM and Area Commanders (future OPCOM) via chain of command.

5. Sponsors shall:
 - a. Develop and communicate requirements in the product's Operational Requirements Document (ORD). Communicate the ORD and all ORD changes, to the acquisition agents, sustainment agents, the operator representatives and user representatives.
 - b. Ensure that all product requirements are quantifiable and identifiable.
 - c. Validate that the specifications developed by the acquisition agents, sustainment agents, operator representatives and user representatives; meet the sponsor's requirements.
 - d. Chair the CCB for changes to the functional requirements in the configuration baseline, which shall be defined in the ORD.

6. CCBs shall:
 - a. Have authority over changes, variance request and problem report actions, for assets and the associated configuration baselines under their change control authority.
 - b. Include as its stake holders: acquisition agents, sustainment agents, operator representatives, user representatives and the Sponsor.
 - c. Either achieve unanimous consent or document the non-concurrence (who non-concurred, the reason for non-concurrence, the justification for overriding the unanimous consent requirement and the actions taken to mitigate risk that may have been identified by the non-concurring party).
 - d. Be chaired by the sponsor for changes to the functional requirements in the baseline, which shall be defined in the ORD. For other changes, the acquisition agent shall chair the CCB during acquisition and the sustainment agent shall chair the CCB during sustainment.

The authority and responsibilities of the CCB Chair shall include:

 - (1) Ensuring that the CCB operates in accordance with the Configuration Management Plan.
 - (2) Ensuring that resources are committed to implement approved changes.
 - (3) Making final decisions on change request, variance request and problem reports, when unanimous consent is not achieved.
 - (4) Ensuring that CCB decisions balance effective operations and efficient use of resources.
 - e. Evaluate proposed configuration changes, variance request and problem reports, and make dispositions in a timely fashion.
 - f. Identify and resolve issues impacting multiple CCBs including those that cross Directorates, platforms, systems and interfaces. Refer unresolved issues between CCBs to the next higher level CCB or common authority in the command structure.
 - g. Track the request and disposition of all changes submitted to the CCB.
 - h. If authorized by their charter, charter subordinate or Local CCBs as needed for specific products.

- i. Prior to approving any request for change, identify appropriate funding source(s) and verify commitment of funds to the approved change
 - j. Have limited authority to approve changes based on the following:
 - (1) Wherever there is a hierarchy of CCBs on a complex program, authority may be limited by a higher level CCB.
 - (2) Local CCBs shall not approve changes for documents and products for which they do not have controlling authority, unless they are instructed to do so by the CCB with controlling authority.
 - (3) The USN/USCG Permanent Joint Working Group (NAVGARD BOARD) must approve all changes to NTNO assets.
 - (4) The potential impact on other CCBs. In this case, the CCB that receives the change request shall either achieve unanimous consent among all affected CCBs or document the non-concurrence (who non-concurred, the reason for non-concurrence, the justification for overriding the unanimous consent requirement and the actions taken to mitigate risk that may have been identified by the non-concurring party).
7. Configuration Managers shall perform the following functions:
- a. CM Planning and Management - Support the program/product line in development of the CM Plan and CCB Charter.
 - b. Configuration Identification - Ensure that Configuration Identification is performed in accordance with the standard CM processes and the CM Plan.
 - c. Status Accounting
 - (1) Record approved, pending and disapproved status of configuration documentation and identifiers associated with assigned products.
 - (2) Record and report to the Chief of Staff (future DCMS), FORCECOM and Area Commanders (future OPCOM) via chain of command; the status of proposed changes from initiation to final disposition.
 - d. Change Control
 - (1) Ensure that prior to CCB meetings, CCBs have the information required to evaluate proposed changes, including but not limited to technical merit, cost, and the impact on operations, schedule, and life cycle sustainment.
 - (2) Record and report the status of all change requests, variance request and problem report that affect configurations.
 - (3) Provide traceability of all changes from the originally released configuration documentation.
 - (4) Record and report implementation status of approved changes.
 - (5) Record and report the affectivity and implementation status of configuration changes.

- e. Audit and Verification
 - (1) Participate in and provide information for audits of assigned products.
 - (2) Track and report the results of configuration audits including the status, corrective action owner, expected completion date, final disposition of identified discrepancies and root cause closed loop corrective action items.
 - (3) Report summary results of configuration audits to Commandant (CG-444), including all unauthorized changes and the associated cost.
- 8. CM Verification and Audit Teams shall:
 - a. Review processes and products to validate compliance with requirements.
 - b. Verify that products conform to released documentation, requirements and design specifications.
 - c. Notify appropriate Logistics and Service Centers and the unit's ADCON for action regarding any audit non-conformances and whether the non-conformances were corrected during the audit. Provide same notification for information to the Chief of Staff (future DCMS), FORCECOM and Area Commanders (future OPCOM) via chain of command.
- 9. FORCECOM shall, in conjunction with Commandant (CG-444), develop, implement, and carry out an audit program to ensure configuration management is being effectively maintained throughout the CG.

CONFIGURATION MANAGEMENT PRINCIPLES

The following are key CM principles from reference (a), EIA-649-A National Consensus Standard for Configuration Management:

1. Management and Planning – There shall be a CM plan defining how to:
 - a. PRINCIPLE 1-1. Identify the context and environment for a product to which CM is to be applied to determine specific CM application methods and levels of emphasis.
 - b. PRINCIPLE 1-2. Document how the Organization will implement CM functions to provide consistency among the product requirements, the product's configuration information, and the product throughout the applicable phases of the product's lifecycle.
 - c. PRINCIPLE 1-3. Identify resources required to implement the CM functions and ensure they are applied throughout the product's life cycle.
 - d. PRINCIPLE 1-4. Establish procedures to define how each CM function will be accomplished.
 - e. PRINCIPLE 1-5. Conduct training so that individuals understand their responsibility, authority, accountability, and the procedures for performing specified CM tasks.
 - f. PRINCIPLE 1-6. Use performance measures to assess the CM plan in terms of implementation and the effective performance of CM functions.
 - g. PRINCIPLE 1-7. Delegate appropriate CM requirements to suppliers and monitor for CM functional performance.
 - h. PRINCIPLE 1-8A. Establish product configuration information status levels.
 - i. PRINCIPLE 1-8B. Ensure that transmitted product configuration information is usable.
 - j. PRINCIPLE 1-9. Plan for long-term data preservation by addressing the information technologies used to store, retrieve, and interpret data.
2. The Configuration Identification shall:
 - a. PRINCIPLE 2-1. Define the attributes of a product and its interfaces in the product definition information and use it as the basis for product operational information.
 - b. PRINCIPLE 2-2. Define a product composition which matches its Product Configuration Information.
 - c. PRINCIPLE 2-3A. Use enterprise identifiers on products as well as related product configuration information, to designate the responsible designer or manufacturer.
 - d. PRINCIPLE 2-3B. Assign unique identification to products.
 - e. PRINCIPLE 2-3C. Change product identifiers to reflect a revision to the product configuration.
 - f. PRINCIPLE 2-3D. Assign a unique unit identifier to individual units of a product when there is a need to distinguish one unit of the product from another.

- g. PRINCIPLE 2-3E. Assign a unique product group identifier to a series of like units of a product when it is unnecessary to identify individual units.
 - h. PRINCIPLE 2-3F. Uniquely identify product configuration information so that it can be correctly associated with the applicable product.
 - i. PRINCIPLE 2-4A. Establish each baseline by approving the stated definition of a product's attributes.
 - j. PRINCIPLE 2-4B. Define each configuration baseline by approving product definition information at a point in time providing a known configuration from which changes are addressed.
 - k. PRINCIPLE 2-4C. Update the current configuration baseline by incorporating any approved change into the previously approved baseline. Retain prior configuration baselines as appropriate.
 - l. PRINCIPLE 2-5. Identify interfaces and establish mutually agreed-to control of common attributes for product boundaries.
3. Change Control processes shall be defined and implemented that:
- a. PRINCIPLE 3-1A. Establish criteria for initiating requests for change to assure changes add value.
 - b. PRINCIPLE 3-1B. Document and uniquely identify each request for change.
 - c. PRINCIPLE 3-1C. Classify requested changes to aid in determining the appropriate levels of review and approval.
 - d. PRINCIPLE 3-2A. Evaluate the technical, support, schedule, and cost impacts of a requested change before approval or implementation or incorporation in the product or product configuration information.
 - e. PRINCIPLE 3-2B. Assess potential effects of a change and coordinate impacts with the impacted areas of responsibility.
 - f. PRINCIPLE 3-2C. Determine the affectivity of a change so that the total impacts of the change can be quantified and the change can be priced and scheduled.
 - g. PRINCIPLE 3-2D. Ensure the decision maker is aware of the complete cost impact of the change.
 - h. PRINCIPLE 3-2E. Identify an appropriate change approval authority that can approve any change and commit resources for implementation.
 - i. PRINCIPLE 3-3A. Implement each approved change in accordance with the approved change information.
 - j. PRINCIPLE 3-3B. Coordinate change implementation with support, maintenance and all other impacted areas before and during change implementation.
 - k. PRINCIPLE 3-3C. Verify implementation of a change to ensure consistency among the product, the product configuration information and the product support elements.

1. PRINCIPLE 3-4. Document and use the appropriate level of authority to approve any temporary departures from approved configurations.

4. Configuration Status Accounting (CSA) processes shall be defined and implemented that:
 - a. PRINCIPLE 4-1A. Systematically capture, record, safeguard, validate, and disseminate data about the product and product configuration information.
 - b. PRINCIPLE 4-1B. Capture data about the product configuration and the product configuration information as it is created over the product life cycle.
 - c. PRINCIPLE 4-1C. Provide controlled access to CSA information.
 - d. PRINCIPLE 4-2. Determine the system requirements for data collection and information processing based upon the need for data about the product configuration and the product configuration information.

5. Verification and Audit processes shall be defined and implemented that:
 - a. PRINCIPLE 5-1. Verify the product's baseline performance attributes through a systematic comparison with the results of associated product tests, analyses, inspections, demonstrations and simulations.
 - b. PRINCIPLE 5-2. Verify that a product's design attributes are accurately reflected in the product definition information.
 - c. PRINCIPLE 5-3. Maintain surveillance over the configuration management process to ensure that the process is adequately documented, that the process documentation is being followed and that the process execution is in compliance with requirements.

KEY DEFINITIONS

1. **Asset:** An aggregation or system of CIs. An alias for configuration item or product. Something that is used or produced to satisfy a need or is the result of a process and determined to be worthy of configuration management. Examples include, but are not limited to: boats, cutters, aircraft, C4IT systems, people (billet structures, certification requirements and documentation), business processes, financial processes, information systems, hardware, software, data, platforms, facilities and equipment.
2. **Acquisition agent:** The organizational element responsible for the acquisitions of an asset or product.
3. **Configuration baseline (or baseline):** Agreed-to information that identifies and establishes the attributes of a product at a point in time and that serves as basis for defining change.
4. **Configuration Identification:** The CM function which establishes a structure for products and product configuration information.
5. **Configuration Item (CI):** Something that satisfies an end use function and is designated for separate configuration management. A CI may also be an aggregation of a system of subordinate CIs or an alias for product.
6. **Configuration Management (CM):** A process for meeting requirements and accommodating change. CM establishes and maintains the consistency of a product's performance, functional, logical, and physical attributes with its requirements, design, and operational information throughout its life cycle.
7. **Configuration Status Accounting:** The CM activity concerning capture, storage, and access to configuration information needed to effectively manage products and product information.
8. **Logistics and Service Centers:** Part of the bi-level structure of the Chief of Staff (future Deputy Commandant for Mission Support (DCMS) organization. A centralized point for providing support services. All support services not accomplished at the unit level are coordinated and managed through these centers.
9. **Product:** See Asset.
10. **Root Cause Closed Loop Corrective Action:** A set of process improvement actions that document, verify and diagnose non-conformances and prevents them from reoccurring.
11. **Sponsor:** The organizational element that defines requirements and accepts capability needed to support a CG mission or business function.
12. **Sustainment agent:** The organizational element responsible for maintenance, support, and availability of an asset or product.