U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

US Coast Guard Stop 7714
2703 Martin Luther King Jr. Ave SE
Washington DC 20593-7714
Staff Symbol: CG-444
Phone: (202) 475-5645

COMDTINST 4130.6C
17 APR 2019

COMMANDANT INSTRUCTION 4130.6C

Subj: COAST GUARD CONFIGURATION MANAGEMENT POLICY

Ref: (a) Department of Homeland Security Configuration Management Policy, CM000001-01 (series)

1. PURPOSE. This Instruction establishes the Coast Guard Configuration Management (CM) Program as required by Reference (a). The CM program uses a multi-layered structure within the Coast Guard (CG) enterprise for leading, governing, integrating, and managing CM functions. This policy must be used in concert with the Configuration Manager's Handbook.

2. ACTION. All CG unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements must comply with the provisions of this Instruction. Internet release is authorized.

3. DIRECTIVES AFFECTED. The following directive is hereby cancelled: Coast Guard Configuration Management Manual, COMDTINST M4130.6B.

4. DISCUSSION. This Instruction and its associated guidance as contained in the CM Manager's Handbook applies to all existing and new start CG configurations, including computer software and firmware. Implementation must be in accordance with the process and procedures specified in the CM Manager's Handbook.

5. DISCLAIMER. This guidance and associated guidance as contained in the CM Manager's Handbook are intended to provide operational requirements for Coast Guard personnel only and is not intended to, nor does it, impose legally-binding requirements on any party outside the Coast Guard.

6. MAJOR CHANGES. This Instruction has been developed by splitting the CG Configuration Management Manual, COMDTINST M4130.6B into the CG Configuration Management Policy, COMDTINST 4130.6C and the CM Manager's Handbook.

DISTRIBUTION – SDL No. 169

	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																										
B	X	X	X			X		X	X		X	X	X	X		X		X			X	X			X	
C									X							X	X									
D	X												X													
E										X																
F																										
G																										
H		X				X	X																			

NON-STANDARD DISTRIBUTION:

7. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.

   a. The development of this Instruction and the general policies contained within it have been thoroughly reviewed by the originating office in conjunction with the Office of Environmental Management, Commandant (CG-47). This Instruction is categorically excluded under current Department of Homeland Security (DHS) categorical exclusion (CATEX) A3 from further environmental analysis in accordance with "Implementation of the National Environmental Policy Act (NEPA), DHS Instruction Manual 023-01-001-01 (series).

   b. This Instruction will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policy in this Instruction must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), Department of Homeland Security (DHS) and Coast Guard NEPA policy, and compliance with all other applicable environmental mandates.

8. DISTRIBUTION. No paper distribution will be made of this Instruction and the CM Manager's Handbook. An electronic version will be located on the following Commandant (CG-612) web sites. Internet: http://www.dcms.uscg.mil/directives/, and CG Portal: https://cgportal2.uscg.mil/library/directives/SitePages/Home.aspx. An electronic version of the CM Manager's Handbook will be located on the Commandant (CG-444) CG Portal website: https://cg.portal.uscg.mil/units/cg444/CM%20Policy%20%20Document/Forms/AllItems.aspx.

9. RECORDS MANAGEMENT CONSIDERATIONS. This Instruction has been thoroughly reviewed during the directives clearance process, and it has been determined there are further records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., National Archives & Records Administration requirements, and Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does create significant or substantial change to existing records management requirements.

10. OVERVIEW.

   a. Policy, processes and procedures for the CM Program in the U.S. Coast Guard are defined in this Instruction and the CM Manager's Handbook. This Instruction provides high-level CM requirements and the guidance for how those requirements are to be met. The handbook identifies the principles for documenting and managing the products, services, assets, activities, facilities, systems, data, people, and the interoperability thereof (the who, what, when, where, why, and how) necessary to perform CM as the CG. The Policy stated in this Instruction and the processes and procedures addressed in the CM Manager's Handbook shall be followed by all units and commands within the CG organization. Each unit or command is required to use appropriate levels of configuration management and shall establish a tailored CM process for this purpose.

   b. The objective of CM in the CG is to provide a systematic means for establishing, documenting and controlling the configurations of the CG. CG CM policy applies to all information impacting performance, safety, quality, schedule, cost, environment, and/or budget, and provides managers with the ability to regulate operational performance, readiness, total life-cycle costs, contract requirements, schedules and Integrated Logistics Support (ILS).

c. CM is composed of the following five interrelated elements: Management and Planning, Identification, Control, Status Accounting and Verification and Audits. Definitions of the five elements, direction for how to execute the elements and a summary of milestones associated with each lifecycle phase are contained in the CM Manager's Handbook.

d. Configuration Baselines are an agreed upon description of the attributes of a product, at a point in time, which serves as a starting point for controlling configuration. Traditional configuration baselines known as allocated, functional, and product baselines, are associated with milestones in the lifecycle of a Configuration Item (CI). Configuration baselines build upon one another to ensure the CI meets its required performance and the design documentation that produced the system meets the stated performance. Functional and product baselines are designated when the CI's configuration documentation has been audited and deemed to meet its requirements and accurately depict the design. Configuration Management of the item's design protects it from unwarranted and uncontrolled change and avoids degradation of performance. The CM Manager's Handbook provides detailed procedures to establish, control and manage the configuration baselines.

11. POLICY.

a. General

(1) CM will apply to all assets, systems, subsystems, components and infrastructure, herein after called Configuration Items (CIs). CM begins with the identification of a CI's requirements and ends with the decommissioning of configuration items that are no longer used for production or support.

(2) All CG units, program offices, product lines, service centers and logistics centers are required to use appropriate levels of CM in accordance with this Instruction and the guidance contained in the CM Manager's Handbook. All CG units will have tailored CM processes/procedures in place at the proper level.

(3) CG is to maintain rigorous CM over all CIs and their configuration information including but not limited to boats, aircraft, cutters, Command, Control, Communications, Computers, and Information Technology (C4IT) systems, people (billet structures, certification requirements and documentation), plans, business processes, financial processes, information systems, hardware, software, data, platforms, facilities, equipment, (in coordination with the appropriate Navy activities) Navy Type Navy Owned (NTNO), and Navy Type - Coast Guard Owned (NTCO) products, and all contracted CM services (including performance based logistics support), training aids/systems (i.e., engine labs, C4IT systems), curriculum, and electronic performance support systems. CM must be performed by documenting requirements; maintaining consistency between CIs and their respective configuration 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 the CM Manager's Handbook.

(4) No member of the CG is authorized to change the configuration of any CI and respective configuration 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.

(5) CM must be applied by business line, program, product line, platform, systems, and equipment managers, and other supporting managers throughout the life cycle of a configuration item in accordance with this Instruction.

(6) The degree of CM applied must be tailored for consistency with the quantity, size, life cycle phase, complexity, intended use, and mission criticality of the CI involved. CM must be exercised throughout a CI's total life cycle as outlined in the CM Manager's Handbook.

(7) Procurement Request (PR) packages, Requests for Procurement and statements of work used in contracts for design, development, production, construction, or operational support of platforms, systems, and equipment, including computer software and firmware, must incorporate applicable CM requirements.

(8) CG must ensure the integrity of product information and Technical Data. The concepts of Technical Data Management must be established based on the elements and principles expressed in EIA Standard 649.

NOTE: The U.S. Coast Guard CM Manager's Handbook contains supplemental guidance and instructions on Coast Guard CM process implementation. The CM Manager's Handbook is located at the Configuration Management Division (CG-444) unit workspace on the CG Portal: https://cg.portal.uscg.mil/units/cg444/SitePages/CG-444_Home2.aspx

b. Configuration Planning/Management (Element 1)

(1) CM for CG Products and/or Services, including data, information, computer software and firmware, must be an integral part of the CG operating philosophy.

(2) CM should permit the maximum latitude during the initial definition of need as the functional requirements are being identified.

(3) Provisions must be made in the early CM planning and execution stages to ensure that the current configuration identification is always known for each item under configuration control. Configuration change impacts must be properly assessed to support areas such as detailed design, safety, quality, system engineering, training and ILS.

(4) CM tasks must be integrated with organizational strategic plans, acquisition program baselines, and master schedules.

(5) Configuration planning details must be documented in a CM plan and include all resources required to execute CM activities during acquisition and sustainment phases.

(6) A CM plan must be developed and implemented for all configuration items, to include, major and non-major CG programs. CM provisions for contractor furnished lower level-CIs will ordinarily be covered in the Contractor's CM plan.

(7) The CM Plan must be reviewed and updated, at a minimum, prior to entering each program lifecycle phase. It is a living document, updated as significant changes occur in the program, particularly in the acquisition phase and during the implementation of the logistic support strategy in the sustainment phase.

(8) Due to the continuous need for revision, update, and implementation of the CM Plan, the respective concurrent clearance authority, at a minimum, must be comprised of the Program Manager (PM), the Product Line Manager (PLM), the CM Manager (CM Mgr), and as appropriate, the Contracting Officer/Funding Manager (KO/FM). Commandant (CG-444)

maintains technical authority and oversight of all CM Plans. CM Plans must be submitted to Commandant (CG-444) for review and concurrence prior to final issuance.

(9) Changes to a configuration must be developed, approved, and managed within the bounds of the operational requirements of the configuration including the required operating capability and planned operating environment.

(10) Interface agreements must be identified in the CM Plan and updated as required.

c. Configuration Identification (Element 2)

(1) Applicable configuration identification documentation must be developed and maintained throughout the life cycle of all CIs. Each Major/Non-Major program or CI shall have a designated CM Manager who is responsible for the life cycle maintenance and control of the configuration documentation. CI determinations and management should be performed as described in the CM Manager's Handbook.

(2) The selection of an item as a CI must be determined by either the need to control the item's inherent design characteristics, attributes, and performance or the need to control the item's interface with other related items.

(3) Further detail on each CI must include the development of a work breakdown structure and include the assignment of unique identifiers, which identify units, and groups of units in a configuration.

(4) CI and configuration information must be maintained and readily available to all CG CCB members.

(5) For each CI, specifications, and drawings must be considered as the primary baseline artifacts. CI baselines must be maintained in a configuration status accounting system.

(6) The CM Enterprise Architecture (EA) must be considered as a primary baseline artifact for functional lines of business.

(7) In Order for integration to be successful in any program, a well-defined CI, consistent with the design, must be established as early in a project as possible.

(8) A unique identifier must be assigned to each CI designated for formal control.

d. Configuration Status Accounting (CSA) (Element 3)

(1) A CSA process tool for creating and organizing the data necessary for managing a configuration shall be utilized.

(2) The configuration information or status must be available for use by decision-makers over the lifecycle of a CI. All data belonging to CIs must be documented in the CSA system of record. The CSA may be an individual software tool, part of an existing tool, or a combination of records that make up the CSA system. The CSA must be accurate at all times to avoid data obsolescence. Data obsolescence can cause cost, schedule and performance issues as well as add risk to the CI and its users.

(3) The development and operation of CSA systems for products, programs, processes, related systems and equipment, including computer software and firmware shall be performed as defined in the CM Manager's Handbook.

(4) The CSA system must be capable of developing and implementing standardized reports. Accurate information must be promptly reported to a CSA system every time an authorized change is made. This information needs to be maintained down to the lowest managed CI level throughout its operational life for use by all levels of management.

(5) Unauthorized configuration changes to any CI or its associated configuration information are not allowed. However, violations, must be reported and documented to capture the configuration accurately and allow for the appropriate action to be taken. Violators are administratively and financially responsible for restoring these changes to the last approved configuration.

(6) The Asset Project Office (APO), Project Resident Office (PRO), Facility Design Construction Center, or Civil Engineering Unit (CEU), as applicable, shall ensure the accuracy of configuration artifacts and design documentation via design review participation and Technical Authority (TA) coordination, or Contractor oversight for each new system. APO/PRO/CEU involvement must start as early as possible, prior to the issuance of solicitation.

(7) Approved but unfunded changes must be recorded in the CSA for new or replacement CIs or services.

(8) CG-LIMS (Coast Guard-Logistics Information Management System) is expected to take over all CG CSA functions in the near future for all CIs including unit level CIs.

e. Configuration Change Control (Element 4)

(1) A configuration change control process must be established to ensure efficient and effective change proposal processing without impeding design development, production, or operational readiness.

(2) Standardized change management processes and procedures must be developed, maintained, and implemented across the CG organization. Change management processes and procedures to be followed shall be addressed in respective CM Plans.

(3) Cognizant PMs and Government Furnished Equipment (GFE) PLMs must establish CCBs to review and approve or disapprove all proposed configuration changes.

(4) The CCBs must ensure that documentation associated with an approved change to a CI is updated to reflect the appropriate baseline.

(5) CCBs must be established for all CIs. Guidance for developing and establishing a configuration control process and a CCB Charter are provided in the CM Manager's Handbook.

(6) CCB hierarchies must be created and managed. The boundaries of change authority at each level of the CCB hierarchy must be defined and documented. Proposed changes crossing into a higher authority boundary must be presented to the higher level CCB for disposition. An example is a change proposed at a Logistics Center that impacts an operational requirement. This would need to be elevated to the CCB that has configuration control over the operational requirements.

(7) Before convening the CCB and voting on a proposed change, the CCB members must ensure that their reporting Subject Matter Experts have thoroughly evaluated the technical

validity of the proposed change, interface effect on other CIs, impact on engineering areas and logistics support, effect on established delivery schedules during production, life cycle cost effectiveness, and the availability of funds.

f. Configuration Verification and Audits (Element 5)

(1) Audits must be used to perform a final accounting prior to establishing a baseline. The completion of a configuration audit results in establishing a configuration baseline which serves as starting point for controlling change.

(2) Formal change control must be applied to ensure success during final design, Functional Configuration Audit (FCA), Physical Configuration Audit (PCA), production or construction, operations and sustainment.

(3) Configuration baselines must be established for CIs.

(4) FCA must be conducted by the Government prior to acceptance or issuance of a decision to proceed to production and is usually executed on a low rate initial production item. The FCA and PCA shall be conducted on a production representative item and be accomplished prior to approving full rate production.

(5) Both the FCA and PCA can be done iteratively to establish the baseline in phases or to culminate in a larger event.

(6) A final FCA and PCA must be conducted after all testing is complete and data is available demonstrating that the solution meets its requirements.

(7) FCAs and PCAs for systems of systems must not be considered complete until completion of full integration testing.

(8) The PCA is the accounting that the technical data package exactly represents the physical item and must be completed prior to the establishment of the product baseline.

(9) The PM is responsible for insuring the FCA and PCA is scheduled and shall carefully review the contract schedule. The CG Configuration Manager or PM in cooperation with the Contractor must develop the Configuration Audit Agenda for use at the FCA and PCA.

12. RESPONSIBILITIES.

a. Directorates [Commandants (CG-1), (CG-4), (CG-6), (CG-7), (CG-9), and Mission Support Offices (DCMS-34), (DCMS-5) and (DCMS-8)] shall:

(1) Educate its CM workforce, direct and oversee the implementation of the CM policy within their directorates. Establish CCBs and Interface Control Boards (ICB) at their level and as necessary to manage interface control boundaries identified within the interface control specification and review changes impacting more than one platform in accordance with the CM Manager's Handbook.

(2) Direct all CG Managers to maintain CM traceability of their functional requirements, services, and investments using the CG Enterprise Architecture.

(3) Clearly articulate levels of configuration control based on Acquisition Strategy to all program staff. (The Government can only approve changes to the level for which they have authority over the design. For commercial items (COTS) this would only include changes to the Performance Specification. Detailed design changes do not fall within this category.)

(4) Resolve disagreements on proposed changes between PMs or PLMs. When a common technical agreement cannot be reached on a change impacting more than one platform, the proposed change shall be referred to the next higher authority as specified in Section 4 of the CM Manager's Handbook to achieve resolution.

(5) Assign CM responsibilities to appropriate Program Managers within their directorates and ensure proper execution of CM Policy.

(6) Designate Configuration Managers and CCB chairs, at their level, in writing and report the names to Commandant (CG-444).

(7) Ensure that Configuration Managers are trained in standard CM processes.

b. Program Managers shall:

(1) Identify CIs and associated baseline documentation under their direct management.

(2) Develop, implement, and maintain a CM Plan for each CI (platform, system or equipment, including computer software and firmware) under their cognizance using Appendix A of the CM Manager's Handbook as guidance. The CM Plan is to be updated at every major milestone and decision event to transition each CI through its lifecycle phases.

(3) Develop and maintain documentation for all CIs (assets, products and administrative information) owned by the CG and deemed configuration worthy.

(4) Forward the CM Plan, with the exception of classified and business sensitive information to Commandant (CG-444) for review, consent and oversight prior to issuance.

(5) Establish a CCB, assign a CCB Chair and issue a CCB Charter at their level for the CIs under their cognizance.

(6) To ensure interoperability, make certain that input for CCBs from cognizant PMs and PLMs is received and assessed by all parties affected.

(7) Provide representation on all CCBs, as required.

(8) Exercise configuration change control. CM Manager's Handbook provides procedural guidance and details on change control.

(9) Ensure all configuration changes are properly processed, documented, and tracked through completion.

(10) Ensure all contracts and data requirements comply with the CM Manager's Handbook, its references and appendices.

(11) Establish internal CM audit and verification teams and define qualifications for their members.

(12) Ensure that FCAs and PCAs are completed and that all audit findings are resolved prior to acceptance. Procedural guidance for conducting and documenting FCAs and PCAs is provided in Appendices C and D of the CM Manager's Handbook.

(13) Audit CM data for accuracy and periodically verify that approved baselines have not been modified without authority.

(14) Submit requests for exceptions to the specified policy and defined responsibilities of this Instruction through Commandant (CG-444).

(15) Solicit Task Commitment Memoranda assigning personnel from Technical Authorities to represent their functional area for all established CCBs.

c. Area Commanders, District Commanders, Commanding Officers (CO) and Officers in Charge shall:

(1) Report product deficiencies and desired improvements to the acquisition and sustainment agents (PMs or PLMs) in accordance with designated process guides.

(2) Submit requests for deviations or waivers.

(3) Implement only those configuration change requests that are approved by the appropriate level CCB and issued in writing through an approved order (CCB Directive, Time Compliant Technical Order or memo). Tailor as necessary and capture specific processes in the CM Plan.

(4) Make no unauthorized configuration changes to assigned products.

(5) Notify appropriate Logistics, Training and Service Centers for action regarding any unauthorized configuration changes or failure to achieve performance requirements.

(6) Notify appropriate Logistics, Training and Service Centers of safety concerns or failure to achieve performance requirements.

d. Sponsors (Operational Requirements Owners) shall:

(1) Develop, manage, and communicate functional requirements. Communicate requirement changes to fellow sponsors, acquisition and sustainment agents, and user representatives.

(2) Ensure operational and support requirements are included in the preliminary functional configuration baseline.

(3) Participate in Systems Engineering Life Cycle (SELC) reviews established by the acquisition project's SELC Tailoring Plan.

(4) Ensure that all requirements are testable and quantifiable.

(5) Validate that specifications meet the sponsor's and user requirements.

(6) Participate or chair the FCA and PCA to ensure test data verifies and validates that operational requirements have been met.

(7) Review and approve the PCA and FCA reports in coordination with Commandant (CG-444).

e. Configuration Control Boards shall:

(1) Have authority over changes, variance requests, and problem report actions for items under their change control authority.

(2) Include stakeholders: Safety, Operators, Enterprise Architecture representative, Sponsor, Test and Evaluation, and Logistics Center/Service Center.

(3) Achieve unanimous consent on proposed change requests or document the non-concurrence (who did not concur, 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). If non-concurrence is "safety" related, or if the change involves adding/removing capabilities not consistent with the approved operational requirements, the change request must be forwarded to respective higher level CCB for review and approval.

(4) Evaluate proposed configuration changes, variance request and problem reports, and make dispositions in a timely fashion.

(5) Identify and resolve issues impacting multiple CCBs, including Interface Control Working Groups that cross directorates, platforms, systems and interfaces. Refer unresolved issues between CCBs to the higher level CCB or respective authority in the command structure.

(6) Track the request and disposition of all changes submitted to the CCB.

(7) If authorized by the CCB charter, charter subordinate or local CCBs as needed for specific configurations.

(8) Prior to approving any request for change, identify appropriate funding source(s) and verify commitment of funds to the approved change.

(9) Have limited authority to approve changes based on the following:

(a) Wherever there is a hierarchy of CCBs on a complex program, authority may be limited by a higher level CCB.

(b) Local CCBs must not approve changes for documents and configurations for which they do not have controlling authority.

(c) The USN/USCG Permanent Joint Working Group (NAVGARD BOARD) must approve all changes to NTNO assets.

(d) The potential impact on other CCBs. In this case, the CCB that receives the change request should 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).

(e) Interface Control Working Groups may need to be established.

f. Configuration Control Board (CCB) Chair shall:

(1) Ensure that the CCB operates per the CM Plan.

(2) Assign a CCB Secretariat.

(3) Make final decisions on change request, variance request and problem reports, when unanimous consent is not achieved.

(4) Ensure actions are tracked until completed, and

(5) Ensure CCB actions are recorded in the CSA.

g. Configuration Managers shall:

(1) Assist/support PM on CM related issues.

(2) Support the program and product line in development of the CM Plan and CCB Charter.

(3) Ensure that Configuration Identification is performed in accordance with the standard CM processes and the CM Plan.

(4) Conduct Status Accounting by:

(a) Recording approved, pending and disapproved status of configuration documentation and identifiers associated with assigned products.

(b) Recording and reporting via chain of command the status of proposed changes from initiation to final disposition.

(c) Establishing and managing baselines.

(5) Conduct change Control by:

(a) Evaluating Engineering Change Proposals to ensure completeness and CCB's readiness including but not limited to technical merit, cost, and the impact on operations, schedule, and life cycle sustainment.

(b) Recording and reporting the status of all change requests, variance requests and problem reports that affect configurations.

(c) Providing traceability of all changes from the originally released configuration documentation from the mission needs statement to the disposition.

(d) Recording and reporting implementation status of approved changes.

(6) Conduct Configuration audits by:

(a) Planning for and ensuring all configuration audit activities, including contract clauses for Contractor participation or support when required.

1) Establishing audit teams of Technical Experts.

2) Gathering data (test reports, drawings and specifications).

3) Gathering special tools for measuring.

4) Performing audits and provide information for all reviews and audits of assigned products.

(b) Tracking and reporting the results of configuration audits including the status, corrective action, expected completion date, final disposition of identified discrepancies and root cause closed loop corrective action items.

(c) Reporting summary results of configuration audits to Commandant (CG-444), including all unauthorized changes and the associated cost.

(7) Conduct configuration verification by:

(a) Planning and ensuring all verification activities are completed.

1) Establishing verification teams.

2) Pulling Validation Aids (Val-Aids) from Logistics information system if required.

3) Verifying physical item nomenclature against logistics system record.

(b) Tracking and reporting the results of configuration audits including the status, corrective action, expected completion date, final disposition of identified discrepancies and root cause closed loop corrective action items.

h. CM Audit Teams shall:

(1) Conduct audit of processes and products.

(2) Ensure products conform to released documentation, requirements, and design specifications.

(3) Notify Program Configuration Manager and PM of non-conformance.

(4) Oversee audits and verifications delegated to Original Equipment Manufacturers.

(5) Promulgate Audit Report.

(6) Record results in CSA system.

(7) Track findings until remediated.

Audit Team Chairman shall:

(a) Recommend acceptance of the equipment and its documentation, and approval of the Baseline Report, subject to the condition and agreements of the audit.

(b) Recommend rejection of the equipment and its documentation and disapproval of the Baseline Report. Reasons for rejection and disapproval must be fully documented by the Audit team, and the specific deficiencies must be noted for further CG review. Upon completion of the audit an updated Baseline Report or equivalent will be submitted as part of the Audit report.

i. CM Verification Teams shall:

(1) Verify physical item nomenclature matches logistics system data.

(2) Notify appropriate Logistics, Training and Service Centers for action regarding any non-conformances and whether the non-conformances were corrected during the audit.

(3) Update logistics systems as required (Coast Guard Logistics Information Management System (CG-LIMS), Fleet Logistics System (FLS), Asset Logistics Management Information System (ALMIS), Configuration Data Manager Database-Open Architecture (CDMD-OA)).

j. Configuration Data Managers shall:

(1) Enter configuration data provided by Configuration and Product Line managers into the logistics information systems.

(2) Maintain integrity of configuration data within information systems through periodic verifications:

(a) Plan for and ensure all verification activities are completed.

1) Establish verification teams.

2) Pull validation aids (drawings, equipment configuration listings, parts lists) from the logistics information system.

3) Verify physical item nomenclature against logistics system record.

(b) Track and report the results of configuration verifications to the Configuration Manager and PLM

k. Commandant (CG-444) (CG CM Technical Authority representative) shall:

(1) Develop and maintain lifecycle CG CM policy.

(2) Represent the Coast Guard on all external Committees for all matters pertaining to CM.

(3) Provide guidance and Subject Matter Expert (SME) knowledge to CM Managers, PMs, and PLMs on changes to CM policy.

(4) Initiate conducting CM assessments across the Coast Guard enterprise CM programs to ensure that procedures and implementation actions comply with the policy of this Instruction and the CM Manager's Handbook.

(5) Monitor and oversee Coast Guard CSA capability and overall management of CSA data and assist with CSA reporting responsibilities.

(6) Through Logistics Compliance Inspections, monitor the logistics system to ensure that guidelines are being adhered to and logistics information contained in the system is complete and accurate.

(7) Direct and oversee Coast Guard implementation of CM policy set forth in this policy.

(8) Provide CM operating and performance requirements for CM IT systems.

(9) Assist with generating Configuration Managers' personal development plans.

(10) Assist with developing CM Human Capital Strategy.

(11) Utilize certification processes for CM Managers, CM specialists, and technicians.

(12) Manage CM program changes to the enterprise architecture.

(13) Direct CM program execution and control within Commandant (CG-444).

(14) Facilitate CM interoperability with the Product Data Program.

(15) Participate in Program Level CCBs as voting member as required.

l. Respective Contracting Officers and PMs shall:

Include appropriate terms and clauses in the contract to ensure Contractors:

(1) Establish a CM program governing all products and services and specifically identify CM tasking to be executed in support of this effort.

(2) Identify the product or service configuration by the Functional Baseline and Product Baseline. (The Contractor must include in the Functional Baseline all system and

performance specifications, interface specifications, test specifications and reports, and contract requirements.)

(3) Control the hardware and software PCB by Form, Fit, Function, Interchangeability and Interoperability in consonance with the Government maintenance concept.

(4) Document all baselines, ECPs, deviations and waivers in the Contractor's CSA database.

(5) Conduct or support CG conducting PCAs as a formal examination of the as-built configuration of the CI against its design documentation as specified in the contract.

(6) Conduct FCAs as specified in the contract for each CI which a separate development or requirements specification has been created.

(7) Provide the necessary facilities, personnel, and documentation to conduct the audits.

m. CM Assessment Teams shall:

(1) Conduct CM internal assessments of processes and products.

(2) Ensure processes comply with CM Policy.

(3) Notify respective Program CM and PM of non-compliance with CM Policy.

(4) Oversee CM assessments of Programs.

(5) Prepare and submit CM Assessment Report to Commandant (CG-444) for promulgation.

(6) Record results in CSA system.

(7) Track findings until remediated.

(8) Use the U.S. Coast Guard CM Manager's Handbook and CM Assessors' Desk Guide for conducting CM assessments.

13. TRAINING. Computer based CM trainings through the Commandant (CG-444) and CG LMS Portals for the CM Managers/CM Workforce shall be made available by Commandant (CG-444) as required.

14. FORMS/REPORTS. None.

15. REQUEST FOR CHANGES. Recommendations for changes and improvements to this Instruction and associated guidance as contained in the CM Manager's Handbook will be submitted via the chain of command to the CM Division, Commandant (CG-444) using Aeronautical Publication Change Recommendation, Form CG-22. Action/submission/routing of documents will be performed via FAX, Email, GCMS, Upload to a website, First Class mail, First Class Certified mail, and commercial carriers such as FedEx, UPS, etc. Electronic submission should be used to the maximum extent possible. If submitted via US mail or commercial carrier, the least costly service type to meet the required delivery date and/or security requirements will be utilized.

MELVIN W. BOUBOULIS /s/
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Engineering and Logistics