Note: November 2022.

This Directive may no longer be current. Please check with the program office responsible for this Directive to determine if there are any updates or if the Directive is no longer in use.

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

Commandant
United States Coast Guard

Stop 7202.
2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7202
Staff Symbol: DCMS
Phone: (202) 372-4534

COMDTINST 5401.5A
06 MAY 2014

COMMANDANT INSTRUCTION 5401.5A

Subj: COMMANDANT (CG-6) DIRECTORATE AND ASSOCIATED DUTIES

Ref:
(a) Delegation for Information Technology, DHS Delegation Number 04000 Revision Number: 00 of 05 Jun 2012
(b) CCG memo 5400 of 23 Mar 2012, Decision Memo: Organization Modification Request to Establish CG CYBER Command
(c) COMMANDANT (CG-6) memo 5320 of 12 Mar 2013, Computer Network Defense Service Provider (CNDSP) Designation
(d) Major Systems Acquisition Manual (MSAM), COMDTINST M5000.10 (series)
(e) Non-Major Acquisition Process (NMAP) Manual, COMDTINST M5000.11 (series)
(f) Coast Guard acquisition Management Roles & Responsibilities, COMDTINST 5000.12 (series)
(g) Command, Control, Communications, Computers and Information Technology (C4IT) System Development Life Cycle (SDLC) Policy, COMDTINST 5230.66 (series)
(h) U.S. Coast Guard Security and Information Assurance (SIA) Manual, COMDTINST M5500.13 (series)
(i) 29 U.S.C. § 794d, Section 508 of the Rehabilitation Act

1. PURPOSE. This Instruction reaffirms the authority, roles, and responsibilities of the Assistant Commandant for Command, Control, Communications, Computers and Information Technology (CG-6), reaffirms the designation as the Chief Information Officer (CIO) in accordance with reference (a), reflects the stand up of Coast Guard Cyber Command, and clarifies the roles and responsibilities of the Commandant (CG-6) directorate offices.

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.163

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

NON-STANDARD DISTRIBUTION:

3. DIRECTIVES AFFECTED. Establishment of the CG-6 Directorate and Associated Duties, COMDTINST 5401.5 is hereby cancelled.

4. BACKGROUND. The Commandant (CG-6) serves to enhance Coast Guard mission performance through efficient and effective management and oversight of Command, Control, Communications, Computers, and Information Technology (C4IT). The Commandant (CG-6) staff accomplishes this by providing C4IT products and services that deliver accurate information to the right people in a timely manner to effectively accomplish their mission. Commandant (CG-6) responsibilities include management and oversight for all Coast Guard C4IT operational, business, and infrastructure assets.

   a. The Commandant (CG-6) directorate was established prior to the establishment of the Deputy Commandant for Mission Support (DCMS) organization. Since the standup of Commandant (CG-6), the business of managing the Coast Guard's C4IT products and services has significantly matured while the complexity of managing C4IT technology continues to increase. The breadth of the CIO's responsibilities can be misunderstood by headquarters' stakeholders and field units. This Instruction clarifies and provides a high level summary of the primary roles and headquarters-level services provided by Commandant (CG-6) Offices for Coast Guard stakeholders. This Instruction does not list all discrete office functions, but is intended to provide an overview of Commandant (CG-6) roles and duties.

   b. The Assistant Commandant for C4IT (CG-6) has two additional titles that reflect distinct authorities and responsibilities. Commandant (CG-6) is also the Coast Guard CIO with responsibilities that flow directly to the Commandant as well as certain senior officials within the Department of Homeland Security and the Department of Defense for C4IT related reporting. In accordance with reference (b), under the technical control of the Assistant Commandant for Intelligence and Criminal Investigations, Commandant (CG-6) is also an operational commander as Commander, Coast Guard Cyber Command (CG CYBER) with responsibility to Commander, United States Cyber. As a Commander, Commandant (CG-6) has command authority to ensure the effective and efficient operation of Coast Guard computer system networks. To ensure C4IT infrastructure resiliency for Coast Guard mission performance, Commandant (CG-6) designated CG CYBER Command as the Coast Guard Computer Network Defense Service Provider (CNDSP) in reference (c).

5. DISCLAIMER. This document is intended to provide operational requirements for Coast Guard personnel and is not intended to nor does it impose legally-binding requirements on any party outside the Coast Guard.

6. MAJOR CHANGES. Incorporation of CG CYBER and Command, Control, Communications, Computers and Information Technology Service Center (C4ITSC).

7. IMPACT ASSESSMENT. This Instruction is not expected to have any impact on existing operations. No additional resources are necessary to carry out this tasking.

8. 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, and are categorically excluded (CE) under current Coast Guard CE # 33 from further environmental analysis, in accordance with Section 2.B.2. and Figure 2-1 of the National Environmental Policy Act Implementing Procedures and Policy for Considering Environmental Impacts, COMDTINST M16475.1 (series). Because this Instruction contains guidance on, and provisions for, compliance with applicable environmental mandates, Coast Guard categorical exclusion #33 is appropriate.

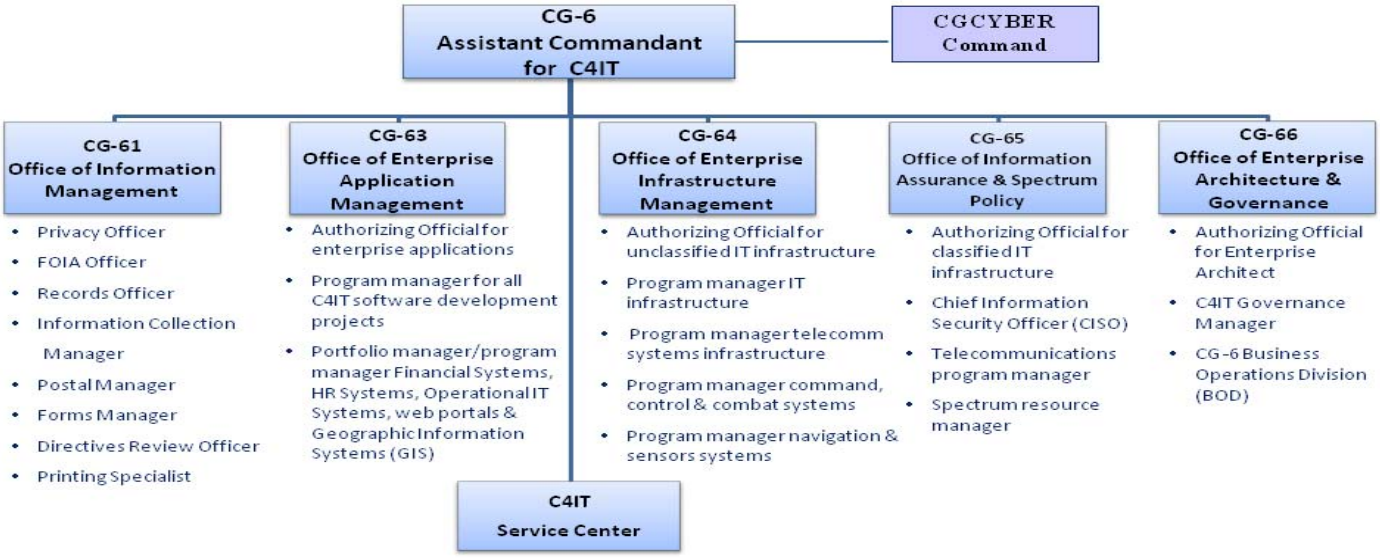
b. This directive will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policies in this Instruction must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), DHS and Coast Guard NEPA policy, and compliance with all other environmental mandates. Due to the administrative and procedural nature of this Instruction, and the environmental guidance provided within it for compliance with all applicable environmental laws prior to promulgating any directive, all applicable environmental considerations are addressed appropriately in this Instruction.

9. DISTRIBUTION. No paper distribution will be made of this Instruction. An electronic version will be located on the following Commandant (CG-612) web sites. Intranet: http://cgweb.comdt.uscg.mil/CGDirectives/Welcome.htm, Internet: http://www.uscg.mil/directives/ , and CGPortal: https://cgportal2.uscg.mil/library/directives/SitePages/Home.aspx

10. RECORDS MANAGEMENT CONSIDERATIONS. This Instruction has been evaluated for potential records management impacts. The development of this Instruction has been thoroughly reviewed during the directives clearance process, and it has been determined there are no further records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., National Archives and Records Administration (NARA) requirements, and the Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does not have any significant or substantial change to existing records management requirements.

11. DEFINITIONS. Commandant (CG-6) will use and adhere to key mission support terms such as Program Management and Technical Authority as defined by DCMS. Specifically, when the terms “program manager” or “programmatic oversight” are used within the context of this Instruction, these terms are separate and distinct from the formal “Program Manager” role or “Program” as defined and used within the acquisition policy references (d) through (f). Where it is necessary to establish Coast Guard definitions for C4IT terminology, Commandant (CG-6) will establish and maintain those definitions on the CG Portal in the document titled “CG-6 Enterprise C4&IT Lexicon” under the CG-6 Enterprise Data Management Program.

12. COMMANDANT (CG-6) ORGANIZATION. Commandant (CG-6) exercises Technical Authority over C4IT. The following organization chart depicts the major Commandant (CG-6) organizational components. Note (1): The office of Enterprise System Development Policy Commandant (CG-69) is not shown below because Commandant (CG-6) has initiated an Organization Modification Request that proposes to realign Commandant (CG-69) functions within Commandant (CG-66). Note (2): Programmatic titles (for example FOIA Officer) identified under each office may be held by a Division Officer, but for brevity have been aggregated under the office titles.



a. As mandated in reference (a), the scope of the CIO's responsibility is very broad. In order to assist the CIO, each Commandant (CG-6) Office holds multiple programmatic titles and performs the following principal, headquarters-level activities:

(1) Policy development, maintenance, and implementation oversight.
(2) C4IT strategy development.
(3) Long-term resource (budget and personnel) planning for operations and sustainment.
(4) Program management of programs assigned to Commandant (CG-6) as CIO.

b. Commandant (CG-6) Offices oversee major C4IT program initiatives as reflected in the CIO's Strategic Plan. This requires that Commandant (CG-6) Offices possess an understanding of the lifecycle cost, schedule, and performance. Embedded and implied within the above specified activities is routine collaboration and communication with external and internal stakeholders which is necessary to influence DHS, Coast Guard, and

DOD policies, plans, and programs that impact the Coast Guard's ability to fulfill its missions and responsibilities as a federal component. Direct management and responsiveness to the myriad of external and internal data-calls is also a principle activity of Commandant (CG-6) Offices with a primary goal of reducing the number and impact of data-calls on field units. For projects not addressed under the major systems acquisition System Engineering Life Cycle (SELC) process, Commandant (CG-6) Offices, especially Commandant (CG-63) and Commandant (CG-64), assist headquarters sponsors through the requirements development process and ensure that the Systems Development Life Cycle process (see reference (g)) is followed.

c. The C4ITSC is responsible for the day-to-day and depot-level C4IT services and mission support activities at agreed upon service levels. The C4ITSC responds to Commandant (CG-6) Office and CG CYBER tasking to execute the CIO's strategic initiatives and policies. Since the CIO is also designated as the Commander of CG CYBER Command, routine collaboration occurs between Commandant (CG-6) Office and CG CYBER staff members to achieve security objectives and develop required policy, plans and strategy.

13. COMMANDANT (CG-6) DIRECTORATE ROLES AND RESPONSIBILITIES. The following roles and responsibilities are associated with the offices within the directorate:

a. **Commandant (CG-61) Office of Information Management**: Provides programmatic oversight of the Coast Guard's Information Management program as established by various laws and regulations including the Federal Records Act, Freedom of Information Act, Privacy Act, and similar legislative mandates. Commandant (CG-61) also directly responds to the Office of Management and Budget (OMB), Department of Justice (DOJ), National Archives and Records Administration (NARA), Department of Homeland Security (DHS), United States Postal Service (USPS), Government Printing Office (GPO) and General Services Administration (GSA) on issues relating to these laws. Commandant (CG-6) functions in the following roles:

(1) Privacy Officer – Commandant (CG-6) Office Chief is the Coast Guard Privacy Officer and is responsible for the Coast Guard Privacy Program. This includes privacy compliance documentation (Privacy Threshold Analysis, Privacy Impact Assessment and Systems of Records Notice) of all information systems and management of all privacy incidents including remediation and mitigation.
(2) Freedom of Information Act (FOIA) Officer – responsible for the Coast Guard FOIA Program including tracking requests, processing appeals, and preparing Congressional responses.
(3) Records Officer – responsible for the Coast Guard Records Program including Presidential mandates.
(4) Information Collection Manager – responsible for the provisions in the Paperwork Reduction Act and publication of notices in the Federal Register.
(5) Postal Manager – responsible for the Coast Guard Postal Program including the Central Postal Account covering equipment, databases, USPS expenditures, DHS Consolidated Remote Delivery System and express services. Also oversees the development of postal security plans during unit relocations.

(6) Forms Manager – responsible for the Coast Guard Forms Program including form design and evaluation, adherence to such laws as the Privacy Act, and conversion of all Coast Guard forms to meet DHS criteria.
(7) Directives Review Officer – responsible for the Coast Guard Directives System including review and approval of all Commandant Directives, ALCOAST messages, and joint services directives.
(8) Printing Specialist – principal administrator and coordinator for all matters pertaining to printing, graphics and reproduction services and primary contact for printing orders through the Government Printing Office.

b. **Commandant (CG-63) Office of Enterprise Applications Management**: Provides programmatic oversight of enterprise-wide Human Resource (HR), Financial, and Operations application portfolios. Commandant (CG-63) functions in the following roles:

(1) Certification and Accreditation Authorizing Official (AO) for enterprise HR, Financial, and Operations systems and applications as described in reference (h) and assigned by the CIO.
(2) Program manager for all enterprise C4IT software development projects including cloud based service applications, data center consolidations, and application integration.
(3) Program manager for HR, Financial, and Operation system portfolios including web portals and Geographic Information Systems (GIS).
(4) Geospatial Management Office (GMO) for enterprise GIS capabilities.
(5) Co-chair of the joint C4, Intelligence, Surveillance and Reconnaissance (C4ISR) and IT Resource Council.

c. **Commandant (CG-64) Office of Enterprise Infrastructure Management:** Provides programmatic oversight of classified and unclassified, enterprise-wide, C4IT integrated systems and C4IT infrastructure. Commandant (CG-64) functions in the following roles:

(1) Certification and accreditation AO for unclassified C4IT infrastructure systems as described in reference (h) and assigned by the CIO.
(2) Program manager for information technology infrastructure that includes standard workstations and associated software, working capital funds, mobility systems, and enterprise services including user authentication and remote access.
(3) Program manager for telecommunication systems infrastructure that includes radio and satellite communications systems, contingency communications systems, Rescue 21, wide area networks and local area networks.
(4) Program manager for command, control and combat systems that includes; command & control systems for ships, aircraft, and shore units; tactical data link communication systems; capital-cutter integrated navigation systems; maritime domain awareness sensors; Vessel Traffic System (VTS) systems, and Nationwide Automatic Identification Systems (NAIS); Navy-Type Navy-Owned (NTNO) and Navy-Type Coast Guard-Owned systems; and combat management systems.
(5) Program manager for navigation & sensors systems that includes Radio-Navigation Transmission & Management Systems (GPS, Differential GPS, Nationwide DGPS), Short Range Aids to Navigation (SRAN), vessel Integrated Navigation Systems

(WLB/WLM Integrated Shipboard Control Systems, Scalable Integrated Navigation Systems), Shipboard Sensors (radar, direction finders, depth sounders), and Optical Sensors (Forward Looking Infrared night vision devices).

(6) Co-chair of the joint C4ISR and IT Resource Council.

d. **Commandant (CG-65) Office of Information Assurance and Spectrum Policy:** Provides programmatic oversight of the Information Assurance (IA), telecommunications, and spectrum resources. Commandant (CG-65) functions in the following roles:

(1) Certification and accreditation AO for classified C4IT infrastructure systems Secret Internet Protocol Router Network (SIPRNET) and GENeral SERvice (GENSER) only as described in reference (h) and assigned by the CIO. Note that AO duties for systems with a Sensitive Compartmented Information caveat are retained within Commandant (CG-2) or other government agencies.
(2) Chief Information Security Officer (CISO) as described in reference (h).
(3) Program manager for the Coast Guard's IA program which includes cyber security.
(4) Program manager for the Coast Guard's telecommunications program and spectrum resources that includes certifications and authorizations to radiate devices on specific frequency assignments within the Coast Guard Communication System; effective communications interoperability with other government agencies, coalition partners, international maritime community; frequency and communications planning; and regulatory equipment authorizations to operate any C4ISR radio communication system.
(5) Coast Guard and US Government representative to national and international communications regulatory and standards bodies including United Nations' International Telecommunications Union (various working parties), International Maritime Organization (Navigation, Communications and SAR subcommittee), International Association for Lighthouse Authorities, Radio Technical Commission for Maritime Services, Global Maritime Distress and Safety System Task Force, interdepartmental and interagency committees, and industry panels.

e. **Commandant (CG-66) Office of Architecture and Governance:** Provides programmatic oversight of the Coast Guard's Enterprise Architecture program. Commandant (CG-66) functions in the following roles:

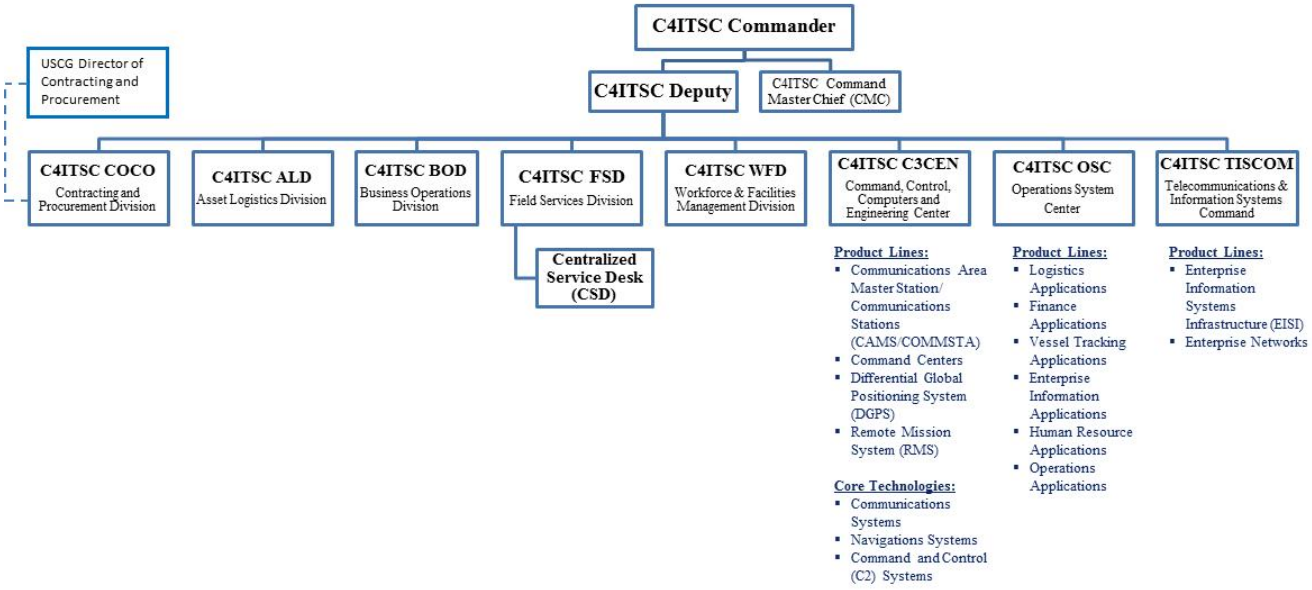
(1) Certification and accreditation AO for enterprise architecture applications (The Enterprise Architecture Management System **(**TEAMS), Dynamic Object Oriented Requirements System (DOORS) and System Architect) as described in reference (h) and assigned by the CIO.
(2) Chief Enterprise Architect.
(3) Program manager for the Coast Guard Enterprise Architecture Program.
(4) C4IT Governance Manager including Chairman of the Enterprise Architecture Board (EAB), Section-508 Coordinator in accordance with reference (i), and IT Acquisition Reviews (ITAR Coordinator).
(5) Commandant (CG-6) Business Operations Division (BOD) including Commandant (CG-6) budget oversight, OMB Exhibits 300 and 53 submissions, Capital Planning and

Investment Control (CPIC) activities, Commandant (CG-6) audit and Congressional-Q response coordinator.

f. **Acquisition Roles and Responsibilities**: The CIO (Commandant (CG-6)) also fills several roles and responsibilities in the major and non-major systems acquisition processes and projects, as outlined in references (d) through (f). These systems acquisition roles and responsibilities include:

(1) Serving as Technical Authorities for C4IT oriented Major System Acquisition Manual (MSAM) and Non-Major Acquisition Program (NMAP) programs, projects, or subprojects.
(2) Working with MSAM/NMAP project requirements Sponsors and MSAM/NMAP acquisition Program and Project Managers for C4IT-related systems and subsystems.
(3) CIO serving as approval authority for MSAM systems engineering life cycle (SELC) technical reviews for major C4IT projects, and Information Technology Acquisition Reviews (ITARs) and Enterprise Architecture Boards (EABs) reviews.

14. C4ITSC ROLES AND RESPONSIBILITIES. Through the Shared Service Divisions (Contracting & Procurement Division(CPD), Asset Logistics Division(ALD), Business Operations Division(BOD), Field Services Division(FSD) & Workforce and Facilities Management Division(WFD)) and the Centers of Excellence (Command, Control & Communications Engineering Center (C3CEN), Operations Systems Center (OSC) and Telecommunication & Information Systems Command (TISCOM)) Product Lines and Core Technologies, the C4ITSC has responsibility for fielding and sustaining C4IT capabilities to standard levels of service. The following organization chart depicts the major components of the C4ITSC.The C4ITSC routinely partners with the Director of Operational Logistics, Force Readiness Command and other Logistic/Service Centers including regular participation in the Director's Council. The C4ITSC issues and maintains C4IT Process Guides that provide guidance to field Information Technology Servicing Organizations (ITSO). The link below hosts the library of C4IT process guides. In the absence of C4IT Standard Operating Procedures issued by the Product Line Managers, C4ITSC Process Guides shall be followed by ITSO throughout the Coast Guard.
https://cgportal2.uscg.mil/units/c4itsc/LibraryProcessGuides/Forms/AllItems.aspx



15. FORMS/REPORTS. None.

16. REQUEST FOR CHANGES. This Instruction will be updated as necessary. Commandant (CG-6) will coordinate the promulgation of time-sensitive amendments when needed. Recommendations for improvement or corrections shall be submitted directly to Commandant (CG-6EA).

MANSON K. BROWN /s/
Vice Admiral, U. S. Coast Guard
Deputy Commandant for Mission Support