U.S. Department of
Homeland Security

United States
Coast Guard

Commandant
United States Coast Guard

US Coast Guard Stop 7710
2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7110
Staff Symbol: CG-6
Phone: (202) 475-3500
Fax: (202) 475-3930
Email: edmp@uscg.mil

COMMANDANT INSTRUCTION 5200.7A

COMDTINST 5200.7A
17 DEC 2018

Subj: COAST GUARD ENTERPRISE DATA MANAGEMENT (EDM) POLICY

Ref:
(a) Department of Homeland Security Enterprise Data Management Directive 103-01 (series)
(b) Commandant (CG-6) Directorate and Associated Duties, COMDTINST 5401.5 (series)
(c) Command, Control, Communications, Computers and Information Technology (C4&IT) Enterprise Architecture (EA) Policy, COMDTINST 5230.68 (series)
(d) Coast Guard Organizational Manual, COMDTINST M5400.7 (series)
(e) Deputy Commandant for Mission Support (DCMS) Engineering Technical Authority (ETA) Policy, COMDTINST 5402.4 (series)
(f) Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Sustainment Management Policy, COMDTINST 5230.72 (series)
(g) Department of Homeland Security Authoritative and Trusted Data Methodology (ATDM)
(h) Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense, DoDI 8320.07 (series)
(i) U.S. Coast Guard Cybersecurity Manual, COMDTINST M5500.13 (series)
(j) National Information Assurance (IA) Glossary, CNSS 4009
(k) National Institute of Standards and Technology Special Publication 800-18 Revision 1 Guide for Developing Security Plans for Federal Information Systems
(l) National Institute of Standards and Technology Special Publication 800-30 Guide for Conducting Risk Assessments
(m) The Coast Guard Freedom of Information (FOIA) and Privacy Acts Manual, COMDTINST M5260.3 (series)

1. PURPOSE. This Instruction establishes the Coast Guard (CG) Enterprise Data Management (EDM) Policy in accordance with Reference (a). It identifies the authority, roles, and responsibilities for governing CG data to ensure compliance with guidance provided in References (b) through (m).

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 policy. Internet release is authorized.

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

NON-STANDARD DISTRIBUTION:

3. DIRECTIVES AFFECTED. The Coast Guard C4I Data Management (DM) Policy, COMDTINST 5200.7 is hereby cancelled.

4. BACKGROUND. Commandant (CG-6) responsibilities include management and oversight of all Coast Guard Command, Control, Communications, Computer, Cyber, and Intelligence (C5I) operational, business, and infrastructure assets. Commandant (CG-6) provides C5I assets that support every CG mission by providing the right information to the right people at the right time to make the right decisions. This is the foundation of having a Ready-Relevant-Responsive Coast Guard. Enterprise data is a valued asset that creates information that can improve mission performance and support decision making. Data leads to information that leads to knowledge, which is information that has been analyzed to provide meaning or value. Information drives command and control decisions. Information supports knowledge management and CG missions and must be shared and reused throughout DoD/DHS and the federal government as an integrated entity. Hence, *information belongs to the enterprise.* In order to accomplish this, consistent data management must be developed and utilized to facilitate the easy retrieval and sharing of information. References (a) through (m) provide the basis for establishing and defining the authority of the CG Enterprise Data Management (EDM) Program while also justifying and rationalizing the objectives of this policy.

   a. Reference (a) establishes and defines the authority of the Department of Homeland Security (DHS) Data Management Policy by the Office of the Chief Information Officer (OCIO). Reference (a) further states that DHS Data Management Policy shall be administered by the DHS Enterprise Data Management Officer (EDMO) under the direction of the DHS OCIO. Reference (a) requires that "Component Chief Information Officers ensure Component compliance with Homeland Security Enterprise Architecture and data management policies and data standards."

   b. Reference (b) establishes and defines the authority, roles, and responsibilities of the Assistant Commandant for Command, Control, Communications, Computers and Information Technology (CG-6) and as the Chief Information Officer (CIO), and it establishes the Assistant Commandant (CG-6) directorate.

   c. Reference (c) establishes and defines the authority of the Coast Guard Enterprise Architecture and assigns responsibility for its governance to the Coast Guard's Chief Enterprise Architect (CEA) on behalf of Assistant Commandant (CG-6) and the U.S. Coast Guard Chief Information Officer (CIO).

   d. References (d) and (e) prescribe the pattern of organization for the Coast Guard and assigns to various components of the organization those functions, which must be performed in order to attain the overall objectives of the Coast Guard. Reference (d) further states that Commandant (CG-67), under the general direction and supervision of the CG-6/CIO, the Chief, Office of Enterprise Architecture & Technology Innovation shall administer the CG Enterprise Data Management Program (EDMP) to guide data quality, sharing, efficiency, security, and compliance.

e. Reference (f) defines the authority, roles, and responsibilities governing the Coast Guard's C5I Sustainment Management for Command, Control, Communications, Computers and Information Technology (C4&IT) systems.

f. Reference (g) defines Authoritative and Trusted Data and component governance process guidelines related to it.

g. Reference (h) establishes policy for sharing of data, information, and information technology services within DoD. It also states that " *The U.S. Coast Guard will adhere to DoD requirements, standards, and policies in this instruction in accordance with the direction in Paragraph 4a of the Memorandum of Agreement between the Department of Defense and the Department of Homeland Security."*

h. Reference (i) defines security policy and roles related to CG Information Technology systems.

i. Reference (j) through (l) define Information Owner roles and responsibilities.

j. Reference (m) sets forth the policy and procedures for administering the Freedom of Information Act (FOIA) and the Privacy Act. It also defines FOIA and Privacy officer role.

5. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide operational guidance 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.

a. This Instruction is renamed from Coast Guard C4I Data Management (DM) Policy to Coast Guard Enterprise Data Management (EDM) Policy. This change emphasizes the goal to correct the perception that data management only applies to C4IT community and that information belongs to the enterprise.

b. Data Sponsor role and responsibilities are assimilated with the Information Owner role and responsibilities to better align with existing DoD guidance.

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 (CE) 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. An electronic version will be located on the Commandant (CG-612) website and Portal:
Internet: http://www.dcms.uscg.mil/directives
CG Portal: https://cg.portal.uscg.mil/library/directives/SitePages/Home.aspx.

9. 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 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.

10. DEFINITIONS.

a. Authoritative Data. Authoritative Data is a specific set of data used to satisfy a business need that has been officially cited or recognized for that need. (Source: Department of Homeland Security Authoritative and Trusted Data Methodology)

b. Authoritative Data Source (ADS). An authoritative data source is the official location and identification ("tagging") to which a specific data element is officially authorized to be created, stored, managed, and destroyed. All other locations are copies of the authoritative data source record. (Source: Department of Homeland Security Authoritative and Trusted Data Methodology)

c. Big Data: Big Data consisits of extensive datasets, primarily in the characteristics of volume, variety, and/or variability, that require a scalable architecture for efficient storage, manipulation, and analysis. (Source: NIST Big Data Interoperability Framework: Volume1, Definitions)

d. Data Management. Data Management is the practice of putting policies, procedures, and best practices into place which ensure data is understandable, trusted, visible, accessible, and interoperable. Data Management functions include processes and procedures that cover planning g, modeling, security, information assurance, access control, and quality. Outcomes of Data Management include the improvement of data quality and assurance, enablement of information sharing, and the fostering of data reuse by minimizing data redundancy. Data management also includes assuring that information confidentiality, integrity, and availability is maintained. (Source: DHS Lexicon)

e. Data Model. Data model supports the development of information systems by providing the definition and format of data. The model consists of entity types, attributes, relationships, integrity rules, and the definitions of those objects. (Source: DHS Lexicon)

f. Data Steward. A Data Steward provides service and leadership with respect to data management, and making decisions based on the enterprise perspective. Data Stewards perform their stewardship responsibilities as an integral part of the duties they are assigned, and as such, their job descriptions shall reflect specific enterprise data responsibilities such as data definition, data quality, data production and/or data usage. (Source: DHS Lexicon)

g. Data Tagging (Metadata). Data tagging is the process to which data is labeled to allow for enhanced indexing, search, and interoperability with other data and applications. (Source: Annex M DHS Enterprise Data Management)

h. Enterprise Data. Is the sum of all data collected, created, used, managed, maintained, shared, and stored by DHS Components, organizations, and programs and warrants stewardship by the appropriate data stewards from the enterprise perspective. (Source: DHS Lexicon)

i. Entity Relationship Diagram (ERD). An ERD illustrates the relationships of data elements within a database including the data element name, format and association to other data elements. (Source: DHS Data Modeling Methodology Guidelines)

j. Trusted Data. Trusted data refers to a particular set of data and its source data asset that are certified as meeting high standards of criteria, including integrity, security, quality, and reliability. Re-stated, trusted designations are applied to both a set of data and the data asset containing it or, its source. (Source: Department of Homeland Security Authoritative and Trusted Data Methodology)

11. ROLES AND RESPONSIBILITIES.

a. Chief Information Officer (CIO). Responsible for information resource management and the execution of this policy.

b. Chief Enterprise Architect (CEA). The CG Chief Enterprise Architect, is designated by Commandant (CG-6)/CIO, as the Program Manager for the CG EDMP and is responsible for the governance of this policy. Also, the CEA is responsible for developing, communicating, and maintaining the Enterprise Data Management procedures including, data architecture, metadata management, data standardization, data governance, performance measurement and improvement under the EDMP. The data architecture is an integral part to the application, technical, and security architectures managed by the CEA and the business architecture managed by the information owner.

c. Enterprise Data Architect. Responsible for oversight and guidance for the enterprise data architecture, including data models and standards, metadata management, data sharing architecture (Data Reference Model (DRM), National Information Exchange Model (NIEM)) and data governance.

d. Data Steward. Responsible for ensuring compliance with the EDM Policy for one or more assigned initiatives. Works with developers to prepare data artifacts needed for governance and decision-making. Prepares data for updating the relevant data catalogs and repositories. Data stewards shall be assigned and shall interface with the roles of associated processes such as the System Engineering Life Cycle (SELC), and Enterprise Architecture Board (EAB), to ensure compliance with data management policy and standards.

e. Freedom of Information and Privacy Acts Officer. Responsible for implementing, overseeing, and providing guidance concerning the Privacy and Freedom of Information Acts, Coast Guard-wide. Works with Information Owners and Data Stewards to assure information is managed in compliance with Freedom of Information and Privacy Acts.

f. Information Owner. Responsible for defining the data requirements, including content, quality and currency, for use in mission operation and/or mission support activities. Information Owners are also responsible for forming and facilitating Communities of Interest (COI) around specific data categories to address differences and issues. As stated in Reference (j), Information Owner is an official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal. The information owner is responsible for managing the business architecture in compliance with CEA defined enterprise architecture standards, capabilities, and requirements.

g. Enterprise Data Management Working Group (EDMWG). The Enterprise Data Management Work Group (EDMWG) shall be chartered under the Enterprise Architecture Board (EAB) by the EAB Chair. The EDMWG shall serve as the CG's Enterprise Data Management Governance Forum, under which the CG's Enterprise Data Management Governance Process shall be conducted. The EDM Governance Process shall serve as the mechanism for addressing EDM issues including changes to the EDM Policy and Practice, and to adjudicate cross-programmatic, and cross-system ATDS functional requirements to ensure they are uniformly applied across systems.

h. Coast Guard Intelligence Chief Data Officer (CGI CDO). This is a dual role of the Coast Guard Deputy CIO for Intelligence. The CGI CDO is responsible for coordination with the Intelligence Community (IC) CIO and IC CDO to ensure CGI data are properly managed within the IC IT Enterprise (IC ITE) architecture as set forth in Intelligence Community Information Environment (IC IE) Data Strategy. This includes ensuring compliance with data standards in the IC Cloud, as well as identification and enforcement of data sharing and safeguarding using Identity, Credential and Access Management (ICAM) capabilities in the IC IE. Ensure CGI needs for Artificial Intelligence and Machine Learning (AI/ML) capabilities can be met by national investments in the Department of Defense (DoD) Joint AI Center (JAIC) and IC Augmenting Intelligence using Machines (AIM) Center, enabled by compliance with these IC standards. Additionally, ensure compliance with data and information management policies and procedures as specified by DHS via the department's Information Sharing and Safeguarding Governance Board (ISSGB).

i. Senior Information Security Officer (SISO). The SISO ensures the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information systems security programs, policies, procedures, and tools. The SISO develops security design requirements through sound design methodology, adequate security control application, and effective configuration practices and ensures secure solutions are incorporated into every aspect of the enterprise supporting an organization's key business processes and organizational mission.

12. POLICY. This Instruction establishes CG Enterprise Data Management policy, implementation, and compliance guidance for References (a) through (m). All Coast Guard Operations and Mission Support organizations involved in creating and using data that support the Coast Guard's missions and/or business operations shall follow this EDM Policy and ensure compliance with the following requirements:

a. All legal requirements and policies including, but not limited to, Freedom of Information Act (FOIA), Privacy Act, Computer Matching and Privacy Act, Records Management, the Federal Information Security Modernizations Act (FISMA), and the Clinger-Cohen Act (CCA), and all applicable legal and policy requirements related to the preservation of data relevant to litigation, security, and References (a) through (m).

b. The creation, quality assurance, change control, use, sharing, efficiency, management, and security of CG data and metadata, whether it is shared or unshared with external entities, shall be conducted in accordance with this EDM Policy and any other existing policies.

c. All operational, mission support, and other required data shall be produced and managed in a manner that is capable of being shared and reused by authorized users with valid mission and business requirements as required by applicable sharing standards.

d. Information system functional requirements shall include a requirement to leverage technology to automatically access and utilize data securely from other available sources or systems wherever possible in lieu of creating and maintaining it themselves. Relying on data sharing as a core tenant will help reduce redundancy, improve data quality, and reduce data management costs while enabling improved mission function.

e. Information system functional requirements shall include a requirement to leverage technology that enables data to meet mobility strategy wherever possible.

f. Information systems shall have Authoritative and Trusted Data Source (ATDS) records to help identify Authoritative and Trusted Data Sets and Sources.

g. Information systems shall identify the authoritative data source location and register identification tags for the data elements stored and/or used by the system.

h. Information systems containing copies of authoritative data shall periodically synchronize an update with authoritative data source for the data elements stored and/or used by the system.

i. Information systems shall minimize the use of copied authoritative data and securely access the authoritative data sources when practicable.

j. Information sharing requirements shall be documented in the EDM Plan to ensure data is shared with authorized users except where limited by law, policy, or classification.

k. Information Owners shall be responsible for assuring that mission operations, mission support, and other data are protected from malicious, deliberate, unintentional, inappropriate, or unauthorized alteration, destruction, access, or disclosure per Reference (i).

l. Existing and emerging CG Data shall be governed by processes established by the EDM Work Group. The EAB shall approve authoritative data sources.

m. All system data shall be modeled, named, and defined consistently across and within the CG in compliance with the References (a), (g), and (h).

n. Synonym names and definitions shall be used as appropriate for end user relevance and understanding. DOD/DHS Lexicon will be the authoritative source for definitions.

o. All Operational, Mission Support, and other data will be tagged with metadata to facilitate data identification, security, access control, sharing and enterprise management. Metadata standards shall include information assurance, quality, privacy sensitivity, security classification, an authoritative source, and business rules for acceptable use for the data.

p. Sources of data that are to be designated as Authoritative and Trusted Data Sources (ATDS) shall be identified, verified, and documented in the Authoritative and Trusted Data Source Questionnaire and registered in the Enterprise System Inventory (ESI) by the Information Owner or Data Steward designated by the Information Owner.

q. ATDS identification, verification, and certification roles, responsibilities, authorities, and processes shall be governed using the mandatory and optional criteria and concepts defined in Sections 3 and 4 of Reference (g).

r. All CG metadata (including ATDS designation) along with data models, Entity Relationship Diagrams (ERDs), tables, fields shall be identified and stored in the CG Enterprise Data Catalog (EDC).

s. Information Owners shall consult Reference (g) to ensure ATDS requirements are addressed in the functional requirements document.

t. Information Owners shall have a designated Data Steward for their system(s) registered within ESI and EDC.

13. IMPLEMENTATION. This Instruction defines the CG EDM Policy. Failure to comply with the requirements of this policy may result in unfavorable consideration in the decision-making including, but not limited to Acquisition Decision Events (ADEs), procurements, resources, and SELC Phase Exit Reviews or no access to or disconnection from the DoD Information Network (DoDIN including CGONE). This Section describes the strategy for EDM implementation:

a. EDM Practice. This policy establishes the authority and responsibility for the Enterprise Architecture Division (CG-671) to publish the EDM Practice Guide. The EDM Practice provides implementation guidance to this policy by describing how to execute the governance, forums, roles, responsibilities, and procedures necessary to ensure compliance with EDM policy requirements described in References (a) through (h).

b. Change Management. The Enterprise Data Management Working Group (EDMWG), consisting of cross-operational and cross-organizational representation shall, under the direction of the Enterprise Architecture Board (EAB), review and update EDM policy and practice.

14. FORMS/REPORTS. None.

15. REQUESTS FOR CHANGES. The Commandant (CG-67) (edmp@uscg.mil) will coordinate changes to this Instruction. This Instruction is under continual review and will be updated as necessary. Time-sensitive amendments will be promulgated via message, pending their inclusion in the next change. All users will provide recommendations for improvement to this Instruction via the chain of command.

D. M. DERMANELIAN /s/
Rear Admiral, U.S. Coast Guard
ASSISTANT COMMANDANT FOR C4IT
(CG-6)