THE COAST GUARD COMMUNICATIONS MANUAL

COMDTINST M2000.3G
October 2021

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 20593-7710
Staff Symbol: CG-6
Phone: (202) 475-3500

COMDTINST M2000.3G
29 OCT 2021

COMMANDANT INSTRUCTION M2000.3G

Subj: COMMUNICATIONS MANUAL

Ref:
(a) Telecommunication Tactics, Techniques, and Procedures, CGTTP 6-01.2 (series)
(b) U.S. Coast Guard Cybersecurity Manual, COMDTINST M5500.13 (series) (FOUO)
(c) U.S. Coast Guard Addendum to the United States National Search and Rescue Supplement (NSS) to the International Aeronautical and Maritime Search and Rescue Manual (IAMSAR), COMDTINST M16130.2 (series)
(d) Spectrum Management Policy and Procedures, COMDTINST M2400.1 (series)
(e) Classified Information Management Program, COMDTINST M5510.23 (series) (FOUO)
(f) Secret Internet Protocol Router Network (SIPRNET) Management Policy, COMDTINST 2070.20 (series) (FOUO)
(g) United States Coast Guard Regulations 1992, COMDTINST M5000.3 (series)
(h) U.S. Coast Guard Sector Organization Manual, COMDTINST M5401.6 (series)
(i) Limited Personal Use of Government Office Equipment and Services, COMDTINST 5375.1 (series)
(j) Physical Security and Force Protection Program, COMDTINST M5530.1 (series)
(k) U.S. Coast Guard TEMPEST Program, COMDTINST M2241.6 (series) (FOUO)
(l) Department of the Navy COMSEC Policy and Procedures Manual (CMS – 1) (series)
(m) Satellite Communications, CJCSI 6250.1 (series)
(n) Personnel Security and Suitability Program, COMDTINST M5520.12 (series)
(o) Naval Communications, NTP 4 (series)
(p) Records and Information Management Program Roles and Responsibilities, COMDTINST 5212.12 (series)
(q) Naval Operational Planning, NWP 5-01 (series)
(r) Aids to Navigation Manual – Administration, COMDTINST M16500.7 (series)
(s) Radiotelephone Handbook, CGTTP 6-01.1 (series)

DISTRIBUTION – SDL No. 170

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

NON-STANDARD DISTRIBUTION: COMAFLOATRAGRU ATLANTIC Norfolk VA, COMAFLOATRAGRUPAC San Diego CA, COMAFLOATRAGRU Mayport FL, COMAFLOATRAGRUMIDPAC Pearl Harbor HI

1. PURPOSE. This Manual establishes policy for the administration, management, and operation of the Coast Guard Communication System (CGCS). Reference (a) provides actionable, step-by-step procedures regarding the various facets of the CGCS and its supporting organization.

2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements must comply with the provisions of this Manual. Internet release is not authorized.

3. DIRECTIVES AFFECTED. The Telecommunications Manual, COMDTINST M2000.3F is cancelled.

4. DISCUSSION. This Manual provides policy pursuant to the use of the Coast Guard's Communication Systems (CGCS). The CGCS links U.S. Coast Guard (CG) assets (e.g., shore units, aircraft, cutters, and boats) to other agencies and organizations throughout the nation and world. It encompasses all radio, satellite, telephone, and network facilities owned, leased, controlled, and/or used by the CG. This includes associated terminal facilities, equipment, and tools. Refer to Reference (a), Telecommunication Tactics, Techniques, and Procedures, CGTTP 6-01.2 (series) for specific guidance on the implementation of policies stemming from this Manual.

5. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it in itself a rule. It is intended to provide 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. Significant changes to this Manual include:

   a. The title of the Manual changed from the Telecommunications Manual to the Communication Manual.

   b. Communications Organization for Commandant (CG-6) is updated per October 2017 approved Organizational Modification Request (OMR).

   c. Added Command, Control, Communications, Computers, Cyber and Information Technology Service Center (C5ISC) organizational hierarchy and systems.

   d. Communications Tactical (COMTAC) publications policies are removed from Chapter 2 of this Manual.

   e. Policies for the acquisition of communications equipment, previously scattered throughout the Manual, are coalesced in a new Chapter 4, Communication Systems Acquisition. This includes new policy pertaining to locally acquired interoperability systems.

   f. The former Shore Unit, Cutter, and Aircraft Communications chapters are combined into Chapter 5, Operational Communications. This Chapter incorporates new policies pertaining to underway Cutter connectivity via commercial satellite systems and revised aircraft radio communication guard requirements.

   g. Chapter 7, Messaging includes policies pertaining to email, chat or other instant messaging services, and text messaging.

   h. Chapter 8, Unit Communications Administration Record Keeping, Inspections and Reports includes additional policy requiring the recording and inclusion of significant chat sessions and/or text communications in the daily communications log.

i. Chapter 9, Communications Plans and Exercises, is new to this Manual and adds new and revised policies pertaining to interoperability with partnering agencies. The chapter includes radio frequency, contingency communications and interoperability plans, memorandums of agreement or understanding with federal, state, tribal, and local agencies, and policies regarding encrypted communications with partner agencies.

j. Policy from previously released (former Commandant (CG-65), now Commandant (CG-672) numbered Telecommunications Policy messages is incorporated into this Manual including:

004/13: 2182 kHz Distress Watchkeeping Termination (Chapter 11)
006/13: COMSEC Monitoring Legal Certifications Reporting Deadline (Chapter 6)
004/14: CG Tactical Communication (TACCOM) Radio Information Technology (IT) Funding Approval (Chapter 4)
002/15: Sharing of CG Type III Advanced Encryption Standard (AES) Keying Material with Other Government Agencies (Chapter 9)
003/15: Restricted CG Aircraft Use of VHF Channel 70 (156.525 MHz) (Chapter 5)
002/16: Command and Control Information Exchange (C2OIX) Address Indicator Group (AIG) Recapitulations (Chapter 7)
003/16: Encrypted Automatic Identification System (EAIS) Keyset Change (Chapter 6)
003/17: Use of INMARSAT Fleet Broad Band (FBB) Satellite Communications and KU Band Systems (Chapter 5)
001/19: Communications Security System (CMS) Policy (Chapter 6)
001/20: Contingency Communications Plan (CCP) (Chapter 9)
002/20: Fleet Broad Band (FBB) Voice usage
003/20: Loss of VHF/UHF radio

7. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.

a. The development of this Manual 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 Manual is categorically excluded under current Department of Homeland Security (DHS) categorical exclusion DHS (CATEX) A3 from further environmental analysis in accordance with the U.S. Coast Guard Environmental Planning Policy, COMDTINST 5090.1 and the Environmental Planning (EP) Implementing Procedures (IP).

b. This Manual 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 Manual must be individually evaluated for compliance with the National Environmental Policy Act (NEPA) and Environmental Effects Abroad of Major Federal Actions, Executive Order 12114, Department of Homeland Security (DHS) NEPA policy, Coast Guard Environmental Planning policy, and compliance with all other applicable environmental mandates. (series).

8. DISTRIBUTION. No paper distribution will be made of this Manual. An electronic version will be located on the following Commandant (CG-612) website: CGPortal: https://cg.portal.uscg.mil/library/directives/SitePages/Home.aspx.
9. RECORDS MANAGEMENT CONSIDERATIONS. Records created as a result of this Manual, regardless of format or media, must be managed in accordance with the records retention schedules located on the Records Resource Center CGPortal site: cg.portal.uscg.mil/units/cg61/CG611/SitePages/Home.aspx.
10. FORMS/REPORTS. The forms referenced in this Manual are available in USCG Electronic Forms on the Standard Workstation or on the CGPortal at https://cg.portal.uscg.mil/library/forms/SitePages/Home.aspx; https://www.dcms.uscg.mil/forms Standard Forms (SF) can be found at: https://www.gsa.gov/reference/forms.
11. SECTION 508. This Manual was created to adhere to Accessibility guidelines and standards as promulgated by the U.S. Access Board. If changes are needed, please communicate with the Coast Guard Section 508 Program Management Office at Section.508@uscg.mil.
12. REQUEST FOR CHANGES. Units and individuals may formally recommend changes through the chain of command using the Coast Guard memorandum. Comments and suggestions from users of this Manual are welcomed. All such correspondence may be emailed to Commandant (CG-672) at: HQS-SMB-CG-672-@USCG.MIL.

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

RECORD OF CHANGES			
CHANGE NUMBER	**DATE OF CHANGE**	**DATE ENTERED**	**BY WHOM ENTERED**

Table of Contents

List of Figures

CHAPTER 1 COMMUNICATION ORGANIZATION

A. General. The Coast Guard Communication System (CGCS) is specified as an essential resource under DHS, providing the means to share mission critical information with other DHS agencies, the Department of Defense (DOD), and Federal, State, local and Tribal law enforcement officials to meet the objectives of defending our nation. Policies in this Manual apply specifically to CGCS.

B. Coast Guard Communication System (CGCS).

1. Definition. The CGCS links U.S. Coast Guard (CG) assets (e.g., shore units, aircraft, cutters, and boats) to other agencies and organizations throughout the nation and world. It encompasses all radio, satellite, telephone, and network facilities owned, leased, controlled, and/or used by the CG. This includes associated terminal facilities, equipment, tools, techniques, and procedures.

2. Mission. The mission of the CGCS is to:

   a. Provide rapid, reliable, secure or protected, and interoperable communications to meet CG operational requirements;

   b. Ensure connectivity, compatibility, and interoperability with the National Command Authority (NCA); and,

   c. Fulfill national and international obligations to provide public maritime safety notices and distress communication services for the safety of life at sea.

C. Program Management Roles and Responsibilities. CGCS program management is a CG headquarters responsibility. It involves the planning, programming, and budgeting for CGCS along with national and international representation of CG interests. The following section lists roles and responsibilities as they relate to the CGCS. Figure 1 illustrates the programmatic control of the CGCS.

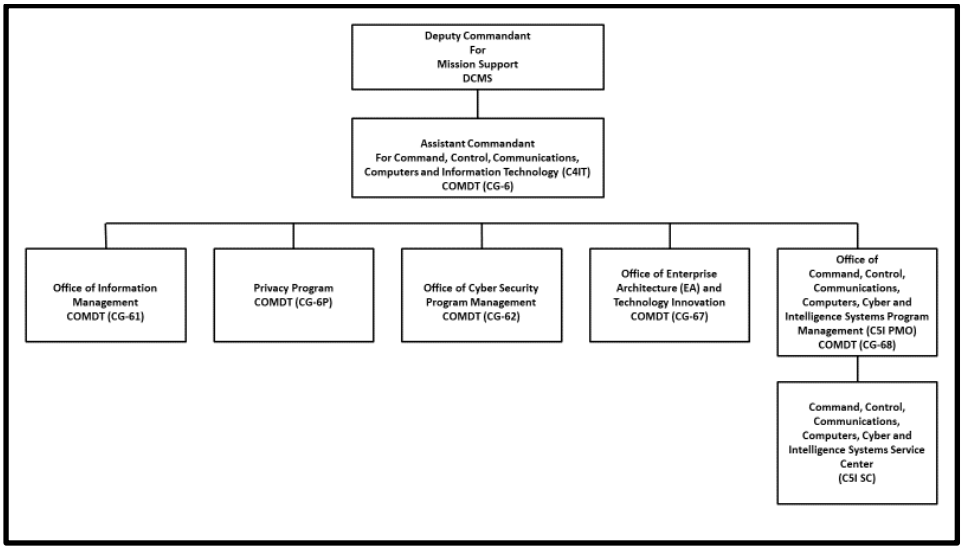

Figure 1 – CGCS Headquarters Programmatic Control

1. Deputy Commandant for Mission Support (DCMS). The Deputy Commandant for Mission Support (DCMS) organization is responsible for all facets of life-cycle management for CG assets, from acquisition through decommissioning. This includes ships, planes, buildings, and information technology.
2. Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (C5IT) (CG-6) and Chief Information Officer (CIO). The mission of Commandant (CG-6) is to enhance C4IT's value in the performance of CG missions by developing and aligning enterprise strategies, policies, and resource decisions with CG strategic goals, mandates, and customer requirements. The CIO serves as the principal staff assistant and senior advisor to the Commandant on matters related to Information Technology (IT) systems and architecture, information resource management (IRM) and efficiencies, cyberspace workforce standards, and cybersecurity standards, in coordination with Commander, CG Cyber Command. Specific roles and responsibilities associated with the Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (C4IT), and (CG-6) are per Command, Control, Communications, Computers, and Information Technology (C4&IT) Investment Management Policy, COMDTINST 5230.71 (series). The following section describes the Commandant (CG-6) organization as it relates to CGCS.
    a. Office of Privacy Management (CG-6P). This office manages the CG Privacy Program to ensure compliance with the Privacy Act and implementing regulations, developing privacy policy, and managing privacy risks.
    b. Office of Information Management, Commandant (CG-61). This office is responsible for program oversight and management of the Coast Guard Information Management program as established by laws and regulations, to include the development and administration of policy for communications records retention.
    c. Cybersecurity Program Management, Commandant (CG-62). This office is responsible for directing and coordinating the CG cybersecurity program, which includes the establishment and management of the CG Risk Management Framework (RMF) in alignment with DoD policies and standards to ensure compliance.
    d. Office of Enterprise Architecture Technology Innovation, Commandant (CG-67). This office is responsible for managing and maintaining program oversight of the CG Enterprise Architecture Program. This office also directs and leads technology communication innovation for the CG, including supporting development of innovative concepts, technology and capabilities to improve capability delivery to support CG mission execution.
        (1) Spectrum Management, and Communications Policy Division Commandant (CG-672). This Division is responsible for the overall regulatory policies of CG electronics, communications, and spectrum management. Commandant (CG-672) also represents the CG in this respect at National and International regulatory bodies such as the National Telecommunications and Information Administration (NTIA) and the Federal Communications Commission (FCC), as well as the United Nations International Maritime Organization (IMO) and International Telecommunication Union (ITU).

(2) Office of Command, Control, Communications, Computers, Cyber and Intelligence Systems (C5I) Program Management, Commandant (CG-68). This office is responsible for programming, planning, resource management, governance, and portfolio management of C5I capabilities for the CG to include the entirety or the communications portfolio of systems.

3. Command, Control, Communications, Computers, Cyber and Information Technology Service Center (C5ISC). The mission of the C5ISC is to enhance C5I value in the performance of CG missions by providing and supporting C5I services that meet mission requirements. The key functions of the Service Center are as follows:

   a. Provide the C5I infrastructure and applications for the execution and support of Coast Guard missions, in accordance with direction, prioritization and guidance from Commandant (CG-68);

   b. Manage C5I Product Lines and shared services over the entire service life cycle, from conceptual planning through disposal;

   c. Develop, test, deliver, and support all C5I systems, applications, and services, to include depot level maintenance planning, execution, reporting, and analysis, in coordination with CGCYBER;

   d. Interface with other Logistics and Service Centers and CGCYBER for the installation, maintenance, and support of C5I services, as required;

   e. Analyze maintenance data to improve reliability, efficiency, effectiveness and cybersecurity;

   f. Ensure C5ISC compliance with the DCMS Mission Support Business Model, including the four pillars of Product Line management, configuration management, total asset visibility, and bi-level maintenance;

   g. Additional information is available on the C5I SC CG Portal site: https://cg.portal.uscg.mil/units/C5ISC/SitePages/Home.aspx.

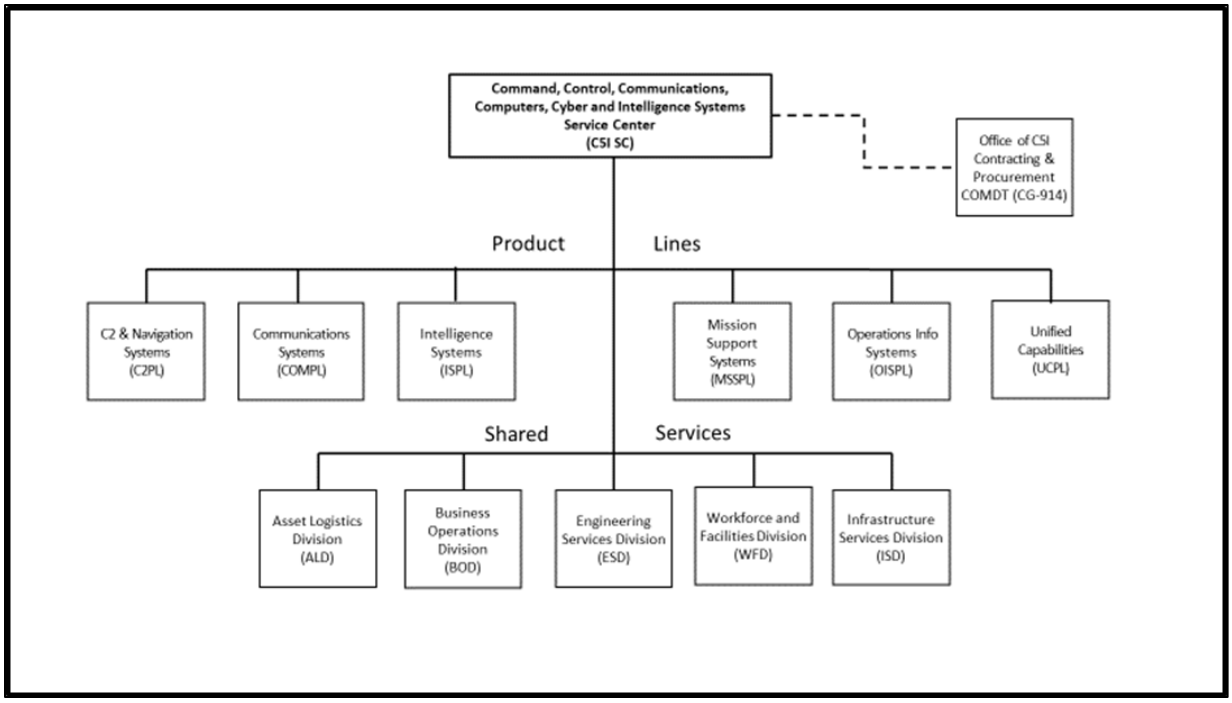

Figure 2 – C5I Service Center Organizational Hierarchy

h. C5I Product Lines. The C5I Product Lines serve as the Service Owner and single point of accountability to provide service development, delivery, support and technical expertise for product line services. Their Key Functions are to manage services in accordance with Service Level Agreements (SLAs); if service levels cannot be met, each product line determines the cause(s) and proposes solutions. The individual product lines establish and manage Operational Level Agreements (OLAs) with any service delivery partners. They oversee and approve all engineering changes and oversee configuration management. Further, they coordinate implementation of new or changed services and support Engineering Analysis Board (EAB) investigations for services as appropriate to determine root cause for failures and to disseminate lessons learned when mishaps and casualties suggest the possibility of being prevented.

i. C5I Shared Services Divisions. Shared services provide the functions and infrastructure that are common across multiple product lines.

4. CGCS Operational Hierarchy. The Deputy Commandant for Operations (DCO) organization uses CGCS for command and control (C2) of CG forces and dissemination of marine safety information to the maritime public. Coast Guard Cyber Command (CYBERCOM) is responsible to operate, monitor and defend CG networks. The following section lists the responsibilities of operational organizations using CGCS. Figure 3 illustrates the CGCS operational hierarchy.

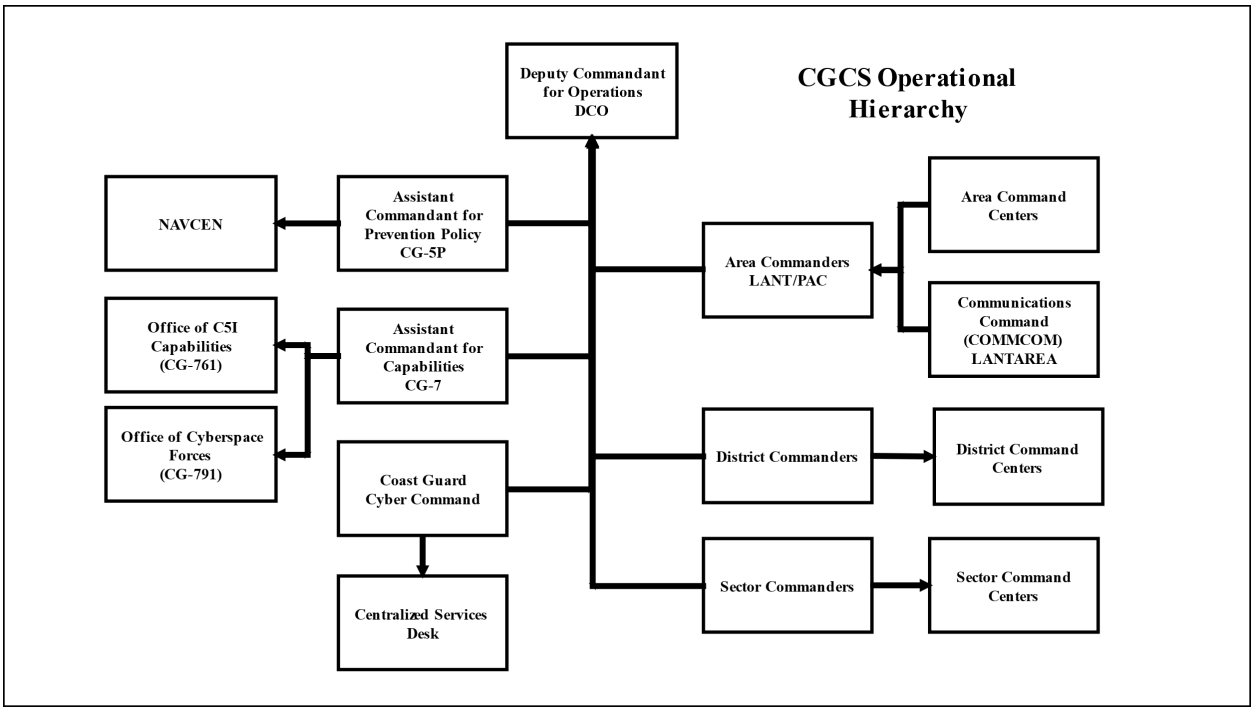

Figure 3 - CGCS Operational Hierarchy

a. Cyber Command. The CG Cyber Command (CGCYBER) serves as the CG component to U.S. Cyber Command. CGCYBER is an operational commander who administratively reports directly to DCO. CGCYBER is responsible for executing cyberspace operations as per DOD, Chairman of the Joint Chiefs of Staff, and CG policy and procedures. The mission of CGCYBER to identify, protect against, enhance resiliency in the face of, and counter electromagnetic threats to CG information and information systems and maritime interests of the U.S., while providing cyber capabilities that foster execution of CG operations, and support DHS and DOD Cyber missions. CGCYBER operates the Cyber Security Operations Center (CSOC), 24 hour a day watch that is the primary computer network defense operational element, protecting CG networks along with the Centralized Service Desk (CSD) which serves as the single point of contact providing 24 hours a day incident and event management for communication equipment, information systems, computers, and electronic systems.

b. Area Commanders. Area Commanders exercise administrative control (ADCON) and operational control (OPCON) of CGCS, less the CGOne Network (CGOne), within their geographic area of responsibility (AOR). This authority involves specifying and assessing the adequacy of communication arrangements, effectiveness of services rendered, and responsiveness in satisfying the operational requirements of all CG operating forces within the Area Commanders' geographic boundaries of responsibility. Specific policies and procedures for operation of CGCS are found in the appropriate Annex K to Area Operations Plan (OPLAN).

c. Atlantic Area (LANTAREA) Chief, C4IT and Security Division (LANT-6) and Pacific Area (PACAREA) Chief, C4IT and Security Division (PAC-6).

(1) Responsible for the operational and administrative oversight of Area and District COMSEC, Information Assurance, information security (INFOSEC), personnel security (PERSEC) and physical security programs.

(2) LANT-6 exercises ADCON and OPCON of the Communications Command (COMMCOM).

(3) Area Commanders can delegate authority to the COMMCOM or Districts to ensure effective system responsiveness, and to:

i. Provide operational direction of the system components;

ii. Coordinate the use of system assets to satisfy the requirements of CG operational units and to provide required services to other government agencies and maritime users of the system; and,

iii. Provide direct liaison with the appropriate Naval Computer and Telecommunications Area Master Station (NCTAMS) for the Area Commander to ensure effective, real time use, and interoperability between the U.S. Navy (USN) and CGCS.

d. Communications Command (COMMCOM). COMMCOM provides rapid, reliable, secure or protected communication services to CG operational commanders, other government agencies, military and civilian organizations throughout the world. See Chapter 5 for details on the specific CGCS services provided by COMMCOM.

e. District Commanders. The Chief, Telecommunications Division or Branch serves as the single point of coordination for identifying operational communication needs within the District's AOR. The District communications office, under the direction of the Commander, must provide communication services for the District office as well as exercise OPCON and ADCON of the CGCS within the district geographic AOR, unless otherwise directed by the Area Commander. The District Command Center (CC) provides command and control of operations and assets within its jurisdiction.

f. Sector Commanders. The Sector Commander is the direct representative of the District commander in all matters pertaining to the CG within the Sector AOR. The Sector commander must provide unified command and control for accomplishing CG missions and objectives. The Sector Command Center (SCC) is the integrator for all operations within a Sector's AOR and the communications unit is the hub for all voice and data communications.

g. Assistant Commandant for Prevention Policy (CG-5P). The Assistant Commandant for Prevention Policy (CG-5P) develops and maintains policy, standards, and program alignment for the prevention activities of the CG to achieve mission success. The directorate oversees the Navigation Center (NAVCEN) and coordinates with National Oceanic and Atmospheric Administration (NOAA) and other government agencies to coordinate maritime safety information dissemination to the public such as weather and urgent marine information broadcasts using CGCS. NAVCEN is the CG Center of Excellence for systems and policy relating to electronic positioning,

navigation, and timing. This includes radio navigation, electronic charting, and vessel identification and tracking. NAVCEN provides the general public with maritime communications information and services on the following web site: https://www.navcen.uscg.gov.

h. Assistant Commandant for Capability (CG-7). The Assistant Commandant for Capability (CG-7) is responsible for identifying and providing capabilities, competencies, and capacity and developing requirements for the staffing, training, equipping, sustaining, maintaining, and employing CG forces to meet mission performance requirements. Operational communication requirements for CGCS are overseen by the Office of Command, Control, Communications, Computers (C4) & Sensors Capabilities (CG-761). Additional discussion of the communication requirements process is provided in Chapter 4 of this Manual.

5. How the organization works. The figures below illustrate the flow of information from the field to CG Headquarters as it pertains to unit requirements, policy issues, and communications spectrum use.

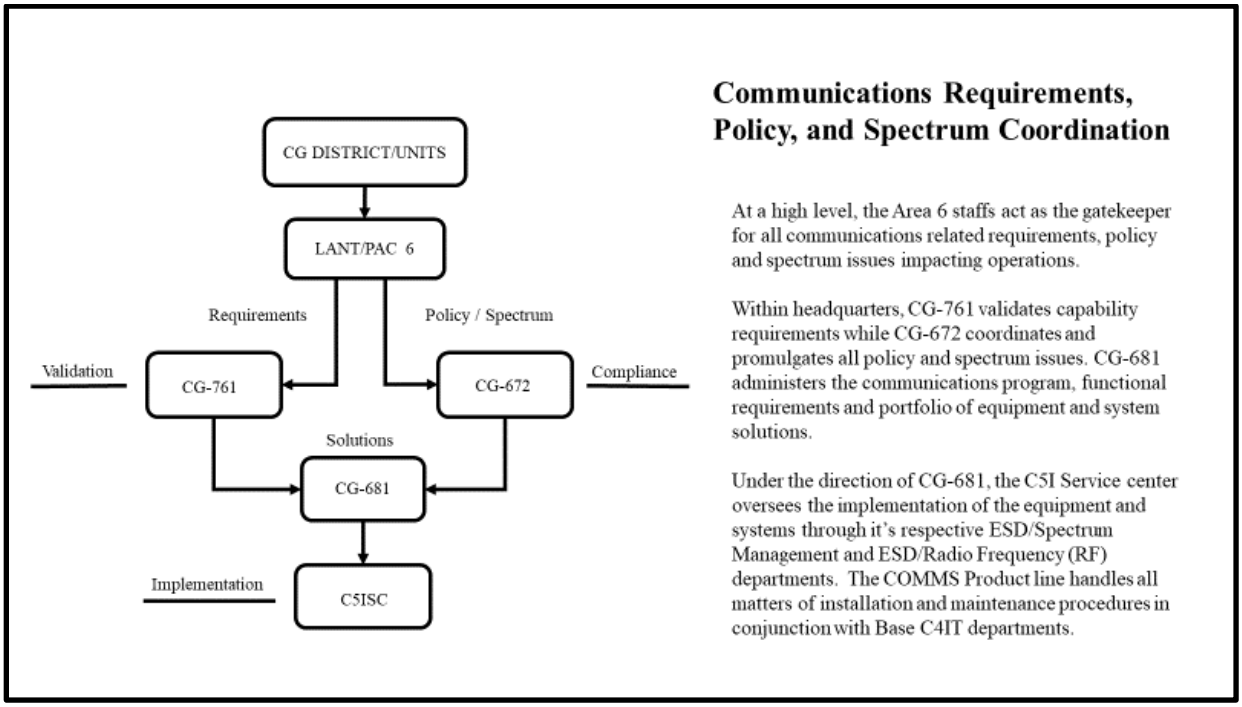

Figure 4 - Communications Requirements, Policy, and Spectrum Coordination

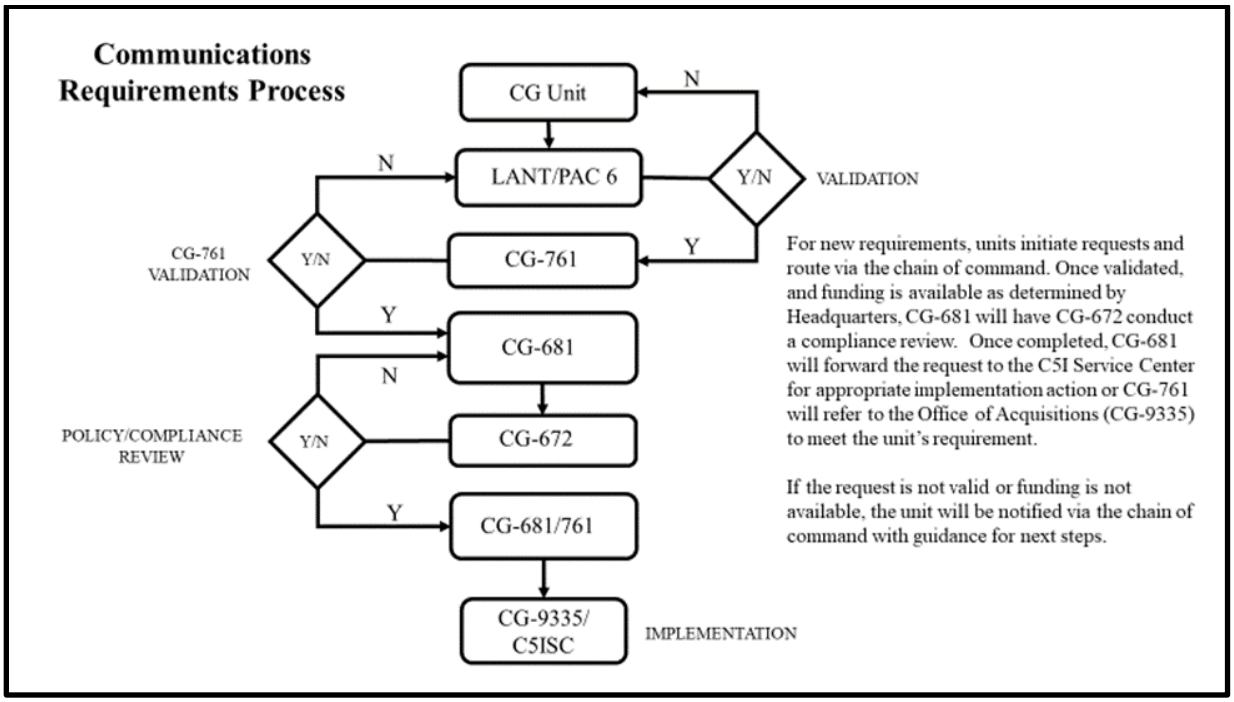

Figure 5 - Communications Requirements Process

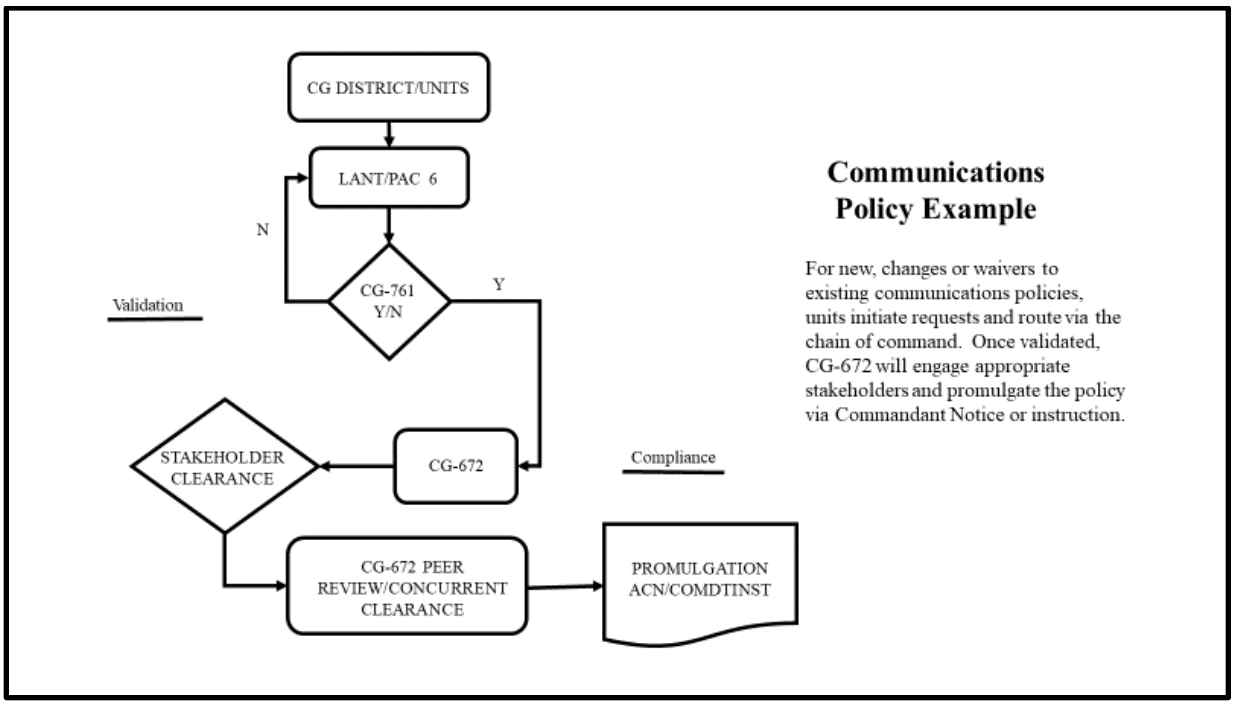

Figure 6 - Communications Policy Change Example

6. Coast Guard Communication System (CGCS) Relationship to Other Organizations. The offices within the Assistant Commandant for Command, Control, Communications, Computers, Cyber and Information Technology (C5IT), Commandant (CG-6) maintain formal relationships and provide liaison with various internal, other federal, and international organizations impacting the CGCS. The CGCS also provides the means for the USN and a variety of law enforcement public safety agencies to communicate and remain interoperable with the CG and DHS. The following sections outline other organizations that support the CGCS.

   a. Assistant Commandant for Intelligence & Criminal Investigations (CG-2). Under the direction and supervision of the Deputy Assistant Commandant for Intelligence and Criminal Investigations (CG-2D), the Chief, Office of Intelligence, Surveillance, and Reconnaissance (ISR) Systems and Technology (CG-26), oversees and manages the USCG ISR Systems and Technology Program, in coordination with the Coast Guard Chief Information Officer (CG-6), the Intelligence Community, DHS, and other Coast Guard program managers.

   b. Cybersecurity and Infrastructure Security Agency's (CISA) Emergency Communications Division. The DHS Emergency Communications Division partners with emergency communications personnel and government officials at all levels to lead the nationwide effort to improve emergency communication capabilities. On July 6, 2012, Executive Order (EO) 13618 was issued to update and clarify national security and emergency preparedness (NS/EP) communication responsibilities for the federal government.

   c. The CG participates in Emergency Communication activities and programs such as the Shared Resources (SHARES) High Frequency Radio Program and the National Emergency Communications Network (NECN). The SHARES and NECN programs function under the DHS Office of Cybersecurity and Communications when activated. Further information on the Presidential Directive providing the authority to execute procedures for continuity of the federal government in the event of a "catastrophic emergency" is in National Security and Homeland Security Presidential Directive NSPD 51/HSPD 20.

   d. Defense Communications System (DCS) and Department of Defense Information Network (DODIN). The DCS and DODIN are composed of the major portions of the individual USN, U.S. Army, and U.S. Air Force worldwide, long haul, point-to-point communication facilities brought together under a single system responsive to the DOD worldwide communication needs. The Defense Information Systems Agency (DISA) exercises OPCON and supervision of the DCS. The respective military departments operate the component facilities. The C5ISC is the principal agent for the CG.

   e. Federal Communications Commission (FCC). The FCC was created by the Communications Act of 1934 and is charged with regulating interstate and international communication by radio, television, wire, satellite, and cable. The FCC furnishes radio direction finding services when requested for search and rescue (SAR) and harmful interference cases. CG units must contact their District

communications offices or Area (LANT-6/PAC-6) staff for spectrum manager liaison with the FCC.

f. National Telecommunications and Information Administration (NTIA). NTIA is an agency of the United States Department of Commerce that serves as the President's principal adviser on telecommunications policies pertaining to the United States' economic and technological advancement and to regulation of the telecommunications industry. NTIA's programs and policymaking focus largely on expanding broadband Internet access and adoption in America, expanding the use of spectrum by all users, and ensuring that the Internet remains an engine for continued innovation and economic growth. The CG leases radio frequency spectrum through the NTIA.

CHAPTER 2 COMMUNICATION GOVERNANCE AND REQUIRED PUBLICATIONS

A. General. CG communications must be conducted per this Manual, federal mandates and policies, International Radio Regulations (IRR), treaties and international agreements, joint and allied/combined communication instructions, Naval Telecommunications Procedures (NTP), Commandant Instructions (COMDTINST), Area and District publications, and directives issued by appropriate authority.

B. Governance.

1. To execute CG duties and functions, the Commandant is authorized to:

   a. Establish, install, abandon, re-establish, reroute, operate, maintain, repair, purchase, or lease such telephone and cables, together with all facilities, apparatus, equipment, structures, appurtenances, accessories, and supplies used or useful in connection with the installation, operation, maintenance, or repair of such lines and cables, including telephones in residences leased or owned by the government of the U.S. when appropriate to assure efficient response to extraordinary operational contingencies of a limited duration, and acquire such real property rights of way, easements, or attachment privileges as may be required for the installation, operation, and maintenance of such lines, cables, and equipment (14 U.S. Code (U.S.C.) § 504(a)(15));

   b. Establish, install, abandon, re-establish, change the location of, operate, maintain, and repair radio transmitting and receiving stations (14 U.S.C. § 504(a)(16)); and

   c. Assist other federal agencies (14 U.S.C. § 701) and to cooperate with National Oceanic and Atmospheric Administration (NOAA) in collecting and disseminating weather information (14 U.S.C. § 707).

2. Commandant (CG-6) supports all CG missions through timely delivery of communication and information technology services. CG operational and administrative communication services and equipment are developed and operate under a broad range of:

   a. Federal laws, regulations, policies, directives and instructions;

   b. Treaties and international agreements, regulations, and equipment standards; and,

   c. Memorandum of Agreement (MOA) and Memorandum of Understanding (MOU) with other federal, state, local, and tribal agencies.

3. In the U.S., maritime communication services are promulgated under the Communications Act of 1934, as amended (47 U.S.C. § 151 et seq.), and the rules and regulations implementing the act adopted by the FCC in title 47 of the Code of Federal Regulations (C.F.R.). 47 C.F.R. Part 80 governs public stations in the Maritime Services. These communications are regulated by two entities:

   a. The FCC regulates public (non-federal) use of the radio spectrum; and

   b. The NTIA regulates federal use of the spectrum.

4. Both public and federal requirements are an integral part of the CGCS. While the CG's internal use of the electromagnetic spectrum (EMS) is regulated by NTIA, FCC requirements placed on public users of the EMS have a direct and significant impact on CG operations. There are numerous requirements imposed on the CG operation of communication facilities, in addition to

the requirements of the Communications Act of 1934, the NTIA, FCC rules and regulations, and International Radio Regulations. The Telecommunications Strategy (TCS), COMDTINST 2000.4 (series), includes a list of primary communications program governance documents.

5. All CG C5I telephony assets, voice, data and video, ship and shore, procured for upgrades, expansions, or replacements must be compliant with Public Law 107-314, DoDI 8100.3, CJCSI 6215.01c, Unified Capabilities Requirement (UCR), UCR 2008 change 2 and Generic Switching Center Requirements (GSCR) 2008.

C. CG Communication Policy Dissemination. The Directives System process will be followed to issue policy changes.

D. Mission Support Policies. Broad communication policies for mission support are listed below. Refer to the noted applicable references as necessary for more specific information dealing with a particular policy.

1. Interagency Policy. Encourage the use of CG communication services by other government agencies, and promote it whenever possible. Coordinate standardized procedures and arrangements at the Area and District level, with appropriate Other Government Agencies (OGA). The OGA requiring communication services is generally expected to reimburse the CG for any additional costs associated with the service.

2. CG-Navy Policy. The Navy Doctrine Library System (NDLS) sets forth joint doctrine to ensure effective communication system support for joint operations. See paragraph F.

3. Inviolability of Information. The CG must maintain inviolability regarding the handling of wire or radio communication information per the Privacy Act of 1974, 5 U.S.C. § 552a. Inviolability, in this case, means that no personally identifiable information (PII), including PII in organization record messages, electronic mail (Email), and/or via voice, may be released or divulged beyond the recipients intended by the originator of the information. Express consent from the originator is required for further dissemination of PII.

4. Health Insurance Portability and Accountability Act of 1996 (HIPAA). The following guidelines apply for the transmission of medical information over CG radios:

   a. HIPAA permits disclosure of patient information for treatment purposes; and

   b. CG members must take precaution when transmitting patient health information to minimize the chance of incidental disclosures.

5. Delivery of Emergency Messages to Private Vessels. The CG has no authority to handle private communication between persons ashore and commercial or private vessels. If a CG unit is asked to deliver a personal message to a vessel, the CG unit must advise the requestor to file the message by commercial means. This does not apply to distress alert message relays.

6. Release of Information Acquired from Communications. The requirements and procedures for the CG to furnish information to the public are set forth in References (a), (b), and (c).
7. Public Service Radio Broadcasts. During a national emergency, natural disaster, or other significant events, CG units are authorized to broadcast public service information, provided the broadcast does not interfere with primary missions.
8. Release of Navigational Information. Per Reference (c), the CG cannot assume responsibility for navigating a vessel, but is authorized to provide the master of a vessel certain published navigational information. Reference (c) provides specific guidance on what information can be provided.
9. Special Authorization for Use of Radio. Use of radio within the territorial waters of any nation falls under the jurisdiction of that nation, and therefore requires authorization for such operations. Per Reference (d), CG use of radio frequencies outside the U.S. & its Possessions (US&P) will be guided by the (ITU) Radio Regulations Table of Frequency Allocations and by the authority of the host government.
    a. Requests for operation of CG fixed sites outside the US&P, including radio frequency assignments, must be submitted six months in advance to Commandant (CG-672). Requests need to be endorsed by the operational commander. See Appendix B of Reference (d) for form and instructions.
    b. Commandant (CG-672) will direct the coordination of any frequency assignment requests outside the US&P with the appropriate governing authorities and through the appropriate U.S. DOD Geographical Combatant Commander (GCC) Joint Frequency Management Office (JFMO).
10. Use of Radio by CG Cutters in Foreign Waters. Permission to transmit must be obtained prior to a foreign port call. A sample foreign port clearance record message is provided in Reference (o). The foreign port clearance record message requires specific information regarding radio requirements of the command.
11. Use of Radio by Foreign Men-of-War in U.S. Waters. As a general rule, foreign men-of-war are allowed to communicate between themselves and with their own governments in privacy, provided they receive the necessary authorization.
    a. These ships must observe the radio regulations currently in effect for the area in which they are operating.
    b. Local naval commanders can withhold authorization if necessary for military reasons and must inform the Chief of Naval Operations (CNO) N3/N6 of such restrictions as soon as practicable and provide the justification for invoking them.
    c. Foreign men-of-war must obtain frequency authorizations in advance through the USN fleet commander sponsoring the visit. The frequency authorization procedures are in Reference (o). If prior arrangements are not made and no USN officer is present, the senior CG officer present must request the cognizant fleet commander grant authorization upon arrival of visiting units.

E. Required Communications Publications. An organization's war fighting and mission publications are a source of information on doctrine, TTP, organizational structures, and employment of equipment. Publications are a means to help facilitate mission accomplishment. CGOne Network provides online access to all required unclassified communication publications. All units using CG record messaging services will maintain ready access to the below listed publications. Cutters will maintain either paper copies or local electronic versions retrievable from onboard computers or stored off line on compact discs or other approved media. The required publications, in addition to this Manual, are:

1. Communications General Instructions, ACP 121 (series);
2. Allied Telecommunications Record System (ALTERS) Operating Procedures, ACP 128 US Supp-1 (series);
3. Naval Telecommunications Procedures Navy Satellite Operations, NTP 2 SEC 1 (series) – WMEC-210' and larger/COMMCOM;
4. Navy Satellite Operations Sec II, NTP 2 SEC 2 (series) – WMEC-210' and larger/COMMCOM;
5. Command and Control Official Information Exchange Manual, NTRP 6-02.3;
6. AIG, CAD, TASK Handbook, NTP 3 SUPP-1 (series);
7. Naval Communications, NTP 4 (series);
8. PROFORMA Message Handbook, NTP 4 SUPP-2 (series);
9. Electromagnetic Spectrum (EMS) Guide, NTP-6 (series);
10. Command, Control, Communications, Computers, and Intelligence (C4I) Infrastructure, NTTP 6-02 (series);
11. Operational Reports, NWP 1-03.1 (series);
12. Navy Planning, NWP 5-01 (series);
13. Cognizant Area Annex K to COMLANTAERA SOP; LANTAREAINST M2000.1 (series) , Annex Kilo (uscg.mil)
14. Telecommunications Tactics, Techniques, and Procedures, CGTTP 6-01.2 (series);
15. The International Code of Signals, (Pub. 102).
16. Navy Tactical Reference Publication, NTRP 1-01 SUPP-2

F. Navy Doctrine Library System (NDLS). North Atlantic Treaty Organization (NATO) publications, Fleet Exercise Publications (FXP), Naval Doctrine Publications (NDP), NTPs, Navy Tactics, Techniques and Procedures (NTTP), Naval Warfare Publications (NWP), and Navy Tactical Reference Publications (NTRP) are accessed through the Navy Doctrine Library System (NDLS). Publications may also include subordinate tactical, Allied and other Joint publications.

G. NATO Publications.

1. The Navy Doctrine Library System (NDLS) serves as the Coast Guard's primary distribution source for NATO publications and is the central control point within a command for administration and maintenance of required NATO publications.

2. The NDLS distributes NATO publications through its online library. The NDLS is supplemented by a collaboration at sea (CAS) library that periodically pushes publication files to shipboard CAS servers and provides Navy Warfare Electronic Library (NWEL) DVD-ROMs produced on demand to fill requests from newly established units and units that cannot obtain what they need online. NDLS and CAS libraries are accessed at the following URLs:
   a. Unclassified NATO publications; https://doctrine.navy.mil/ndls/default.aspx ;
   b. Classified NATO publications; https://doctrine.navy.smil.mil/default.aspx ;
   c. CAS: Local cas server ip/navy/31/site.nsf.
3. Navy Warfare Development Center (NWDC) periodically distributes the Allied Publication Electronic Library (APEL) DVD-ROM. Units receive a two-disc set that contains Allied publications classified up to North Atlantic Treaty Organization (NATO) Confidential. Area Commands must send all requests for NATO classified documents, including the APEL CD set to the Coast Guard NATO Sub-Registry, C5ISC with justification. NATO Secret publications are distributed in paper format to units with an established requirement.
   a. Area Commands must send all requests for NATO classified documents, including the APEL CD set to the Coast Guard NATO Sub-Registry, C5ISC with justification.
   b. Units must comply with Implementation of NATO Security Requirements; United States Security Authority per NATO INST 107 to receive NATO RESTRICTED and NATO CONFIDENTIAL products.
   c. Allied publications and changes must not be implemented by the unit before the specified date. NWDC distributes these documents to units before they become effective so that they are in place when the NATO effective date is announced. The effective date is promulgated via NWDC via a NAVPUB message.
   d. Units must read the NATO letter of promulgation within newly issued NATO publications and changes to find out if they are effective upon receipt or on an effective date specified by NATO.

H. NATO Publication Management.

1. Publications Requirements List (PRL). PRLs are generated based on the units' mission-essential tasks. Units must liaison with Commander, Atlantic Area/Commander, Pacific Area to establish publication requirements for units in their AOR.
2. Safeguarding.
   a. Users must have the appropriate clearance to access classified publications;
   b. Users must safeguard all classified publications per Reference (e).
3. Local Reproduction. Local reproduction consists of any NATO publications downloaded from the NDLS online library to a local or shared file on the unit server. It also includes printing hard copies of NATO publications. Cutters that anticipate intermittent or non-continuous access to the NDLS online library must make local reproductions (either electronic or printed) of required NATO publications prior to getting underway.
   a. All reproductions of classified publications must be done per Reference (e);

b. NATO Publication users must maintain physical custody of any locally produced hard copies.

4. Naval Publication (NAVPUB) Messages. Routine and urgent changes to NATO publications are announced by NAVPUB message and Email to subscribers. NAVPUB messages are listed on the NDLS website. NAVPUB messages are used to announce U.S. and NATO doctrine and tactical publication information. The NAVPUB subscription service on the NDLS website provides commands with Email notification of changes to NATO publications on the NDLS website. Commands with publication requirements must subscribe to the NDLS to receive NAVPUB messages.

I. NATO Publication Security.

1. Security Handling. Users must safeguard, store, investigate, destroy, and report possible or actual loss or compromise of classified NATO publications per Reference (e).

2. Access. NATO publications are available to all users based on their type of network account.

a. Personnel must receive a NATO briefing prior to receiving access to classified allied publications;

b. Classified NATO publications must be protected commensurate with classification of material they contain;

c. For CG personnel, unclassified NATO publications require no special access controls other than on a need to know basis.

J. Foreign Disclosure Program (CG-FDP). Per U.S. Coast Guard Foreign Disclosure Program (CG-FDP), COMDTINST M5260.7 (series) (FOUO), requests for foreign disclosure of classified information or Controlled Unclassified Information (CUI) must be submitted to local Foreign Disclosure Representatives (FDR), or via the chain-of-command to servicing Foreign Disclosure Officers (FDO) at one of the following commands as appropriate:

1. Coast Guard Maritime Intelligence Fusion Center, Atlantic (FDO)

2. Commander, Coast Guard Atlantic Area (LANT-25)

3. Coast Guard Maritime Intelligence Fusion Center, Pacific (FDO)

4. Coast Guard Intelligence Coordination Center (ICC-032)

5. Commandant (CG-222)

CHAPTER 3 COMMUNICATION SYSTEMS

A. General. CGCS includes owned and leased circuits, channels, services, and equipment that provide voice, data, and video teleconferencing services. See Chapter 5, Operational Communications, for specific policies regarding use of CGCS systems.

B. Short Range Radio Systems.

1. National Distress Response System (NDRS). The Very High Frequency (VHF) system established and maintained to provide distress and safety communications for the maritime public, both commercial and recreational and for the promotion of safety on, under, and over the high seas and waters subject to the jurisdiction of the United States by the CG. The primary function of the NDRS is to receive distress alerts, coordinate SAR operations, and communicate with all maritime interest in waters in which the CG has SAR responsibilities. A secondary function is to provide short-range command and control communications for all CG missions.

2. Rescue 21 (RESCUE 21). RESCUE 21 is the current CG implementation of NDRS. RESCUE 21 is a Very High Frequency-Frequency Modulated (VHF-FM) and Ultra High Frequency (UHF) network consisting of transceivers and Remote Fixed Facility (RFF) antenna high-sites remotely controlled by sector communication centers to provide coverage extending out to at least 20 nautical miles from shore. To clarify, the NDRS is the name for the short-range communications function, while RESCUE 21 is the name of the equipment suite used to implement the NDRS function. RESCUE 21 provides sectors, stations and users with clear and/or protected VHF and UHF communication capabilities in addition to direction finding (DF) and digital selective calling (DSC) functions. It is an advanced maritime command, control, communications, and computer (C4) system designed to manage near shore and inland communications for the CG. RESCUE 21 is operational along the Atlantic, Pacific and Gulf coasts of the continental U.S, Western Rivers, and the shores of the Great Lakes and the coasts of Hawaii and several U.S. territories. Modified versions of the system for Alaska have been completed.

3. UHF/VHF Low Sites. UHF and VHF low sites are low elevation, low power radios installed at approved Sectors and stations. CG Sectors and Stations are authorized use of these low sites for local logistics, contingency, and interoperability purposes. The UHF/VHF low sites are not a part of the NDRS system.

4. Nationwide Automatic Identification System (NAIS). NAIS consists of about 134 VHF transceiver sites located throughout the coastal continental U.S., inland rivers, Alaska, Hawaii and Guam. NAIS is designed to collect Automatic Identification System (AIS) transmissions from local vessels. Aboard ship, AIS is a broadcast system that acts like a transponder, operating in the VHF maritime band and serves as a ship-to-ship collision avoidance system. AIS allows for communication of position, speed, and other ship data via a VHF virtual data link (VDL) network.

C. Long Range Radio Systems.

1. High Frequency (HF) Automatic Link Establishment (ALE) Networks. HF ALE command and control networks provide long range voice services to CG Commands, vessels, and aircraft with installed HF ALE equipment. ALE was developed to automatically select the best frequency based on propagation factors with minimal operator assistance. ALE takes the guesswork out of the frequency selection process. Benefits also include automatic signaling, selective calling, automatic handshaking, channel scanning and selection, link quality analysis (LQA), polling, and sounding. Refer to COMMCOM OPGUIDE for operating instructions:

https://cg.portal.uscg.mil/units/commcom/operations/CAT/CAT%20Guides/Forms/AllItems.aspx

2. Cellular Over the Horizon Enforcement Network (COTHEN). DHS Customs and Border Protection (CBP) operates and maintains COTHEN from the National Law Enforcement Communications Center (NLECC) in Orlando, Florida. The COMMCOM has a detachment that is assigned to the NLECC. Utilizing a cryptographic device, COTHEN may be used in a protected mode to handle sensitive, but unclassified (SBU) information. The system may also use Type 1 encryption for classified information, however, NLECC does not support Type 1 encryption. Therefore, prior mission coordination with COMMCOM and/or the unit's Tactical Control (TACON) is required prior to its use in this mode.

3. High Frequency (HF) Digital Selective Calling (DSC). HF DSC is a radiotelephone service to mariners as part of the GMDSS. DSC allows mariners to instantly send an automatically formatted distress alert to the CG or other rescue authority worldwide. DSC also allows mariners to initiate or receive distress, urgency, safety and routine radiotelephone calls to or from any similarly equipped vessel or shore station, without requiring either party to be near a radio loudspeaker.

4. HF Voice.

   a. Sea, Air, Shore Secure (SASS). SASS are available for CG clear and secure HF voice communications for all equipped aircraft, cutters, and shore units. The list of SASS frequencies is promulgated in the OPTASK COMMS by the Area Commander.

   b. Clear voice. The COMMCOM has the capability to communicate over non-secure air-to-ground frequencies. The list of non-secure air-to-ground frequencies is promulgated in the OPTASK COMMS by the Area Commander.

D. Satellite Communication Systems. The CG uses commercial and military satellite communication for daily operations.

1. Commercial Satellite Communication (COMSATCOM). COMSATCOM includes Mobile Satellite Service (MSS), Enhanced Mobile Satellite Service (EMSS), and Fixed Satellite Service (FSS) to provide high quality, rapid wireless voice and data communication links to deployed/mobile units. These services supplement terrestrial command, control, and communication, and can improve interoperability with compatibly equipped Safety of Life at Sea (SOLAS) compliant vessels.

   a. L Band Systems - Inmarsat

      (1) Inmarsat SAILOR 500 Fleet Broadband (FBB). FBB is a maritime global satellite Integrated Services Digital Network (ISDN) network deployed aboard cutters allowing

the terminal to be used anywhere at sea with the exception of the Polar Regions. FBB is a high-cost pay-as-you-use system requiring individual unit monitoring. Units should contact their OPCON for overage authorizations.

(2) Inmarsat Swift 64 and Swift Broadband. Swift 64 and Swift Broadband systems are deployed aboard CG aircraft to provide in flight mobile network connectivity.

(3) Inmarsat-C. Inmarsat-C is a two-way, packet data service, installed aboard cutters. The system is approved for use under the Global Maritime Distress and Safety System (GMDSS) to meet International Maritime Organization (IMO) requirements for the Ship Security Alert Systems.

(4) Inmarsat Broadband Global Area Network (BGAN) Explorer 700. The Inmarsat BGAN Explorer is a manpack sized system used in portable SIPRnet kits (PSK) available through the COMMCOM's Deployable Communication Forces (DCF). They are broadband, multi-user satellite systems of rugged design and provide secure connection to the SIPRnet where necessary in support of operations.

b. Ku Band Systems.

(1) KVH TracPhone. KVH Ku-band systems are employed both afloat and ashore using very small aperture terminals (VSAT) to meet the growing demand for more bandwidth at sea and for deployable operations ashore. In addition, these systems serve as a backup for Rescue 21 terrestrial circuits at a number of remote fixed facilities (RFFs). VSAT provides broadband communications comparable to terrestrial communication data rates ashore. Billing for airtime/use is a monthly flat communication rate, thereby allowing cutters and deployable forces to budget air-time rates without unanticipated charges.

(2) SeaTel. Similar to the TracPhone, SeaTel systems are installed aboard cutters to provide underway connectivity via VSAT terminals. Billing for airtime/use is also a monthly flat communication rate.

c. Iridium Satellite Phones. Iridium satellite phones are a type of mobile phone that connects to satellites instead of phone lines or cellular phone sites. They provide similar functionality to cellular phones including voice, short messaging services, and low bandwidth internet access. The Iridium satellite constellation generally provides for worldwide coverage.

2. Military Satellite Communication (MILSATCOM). USN support to meet MILSATCOM interoperability requirements is outlined in Reference (b). The CG uses both the extremely high frequency (EHF) and UHF frequency bands for MILSATCOM. Operational policies and a list of MILSATCOM circuits authorized for CG are located in Chapter 5 of Reference (b). Operational Unit Communications are promulgated in the OPTASK COMMS by the Area Commander. **NOTE:** DoD Regional Satellite Support Center (RSSC) will issue a unit's Satellite Access Assignment (SAA) mission number via Joint Integrated SATCOM Tool (JIST). A unit experiencing electromagnetic interference (EMI) will be required to submit a Joint Spectrum Interference Resolution Online (JSIRO) identifying the EMI. When a JSIRO is submitted, RSSC will respond by issuing a new or modified SAA. A unit not submitting a JSIRO, RSSC will not take action or issue a new SAA.

E. Data Networks. A data network is a group of interconnected (via cable and/or wireless) computers and peripherals capable of sharing software and hardware resources between many users. CG commands are connected through a wide variety of data networks, public, unclassified, and secure. Data networks are administered and provisioned by the C5ISC and serviced by the regional Base C5I department. The following section is a list of approved CG networks.

1. Department of Homeland Security One Network (DHS OneNet). DHS OneNet is the unclassified wide-area network (WAN) for DHS. DHS OneNet is a multi-protocol label switching (MPLS) network. MPLS is a standards-approved technology that increased network traffic flow. DHS OneNet may be used to process SBU information.
2. Coast Guard One Network (CGOne). CGOne is the CG implementation of DHS OneNet within the .mil domain.
3. Communication Systems Network (CSN). The CSN is a private line network that connects the COMMCOM to its associated radio facilities for remote operations.
4. Internet. The internet is a publicly accessible (non-secure) global system of interconnected computer networks. Reference (b) provides additional policies and guidance on the installation and use of commercially provided internet services at CG facilities. All non-standard internet (i.e., not connected to CGOne) requests will be ordered by the local designated agency representative (DAR) only.
5. Department of Defense Information Networks (DODIN).
    a. Secret Internet Protocol Router Network (SIPRnet). SIPRnet is an enterprise-wide administered WAN. It provides a secure infrastructure for the exchange of voice, video, data, and imagery. SIPRnet is cleared up to the Secret classification level and can be used to process information Secret and below. Although SIPRnet operates similar to the internet, it is a DOD managed secure network limited to authorized U.S. government employees. The SIPRnet WAN is separated from other networks by a combination of physical, procedural, logistical, and cryptographic measures. Please note that in many locations, SIPRnet is "tunneled" through CGOne circuits and will experience simultaneous outage when CGOne services are interrupted.
    b. Non-Classified Internet Protocol Router Network (NIPRnet). NIPRnet is a DOD enterprise WAN that operates at the unclassified level. NIPRNET is DOD's intranet, and provides controlled access to the internet.
    c. Joint Worldwide Intelligence Communications System (JWICS). JWICS is a Defense Intelligence Agency administered enterprise WAN link encrypted internet protocol (IP) network that operates at the Top Secret/Sensitive Compartmented Information (TS/SCI) level for data and video support throughout DOD and other federal agencies. Commandant (CG-26) is responsible for oversight and administration of JWICS throughout the CG enterprise.

F. Telephony Systems. Telephony systems form a critical part of the CG's C5I architecture. Telephony systems include, but are not limited to: commercial telephone service via leased or owned switching equipment, microwave relay systems, Private Branch Exchange (PBX), Voice over Internet Protocol (VoIP), Unified Communications (UC) hardware and software, Video Teleconferencing (VTC) systems, associated peripheral equipment, and cellular telephones.

CHAPTER 4 COMMUNICATION SYSTEMS ACQUISITION

A. General. Acquisition and use of communication services and equipment by federal agencies is subject to significant legal and regulatory restrictions. In addition, to ensure interoperability, security, and sustainability service wide, systems must meet approved standards for installation and use. Therefore, strict communication acquisition management is necessary to ensure the CGCS remains capable of meeting CG mission requirements. Management of acquisition policies and practices by the Assistant Commandant for Command, Control, Communications, Computers and Information Technology, Commandant (CG-6), provides for the sustainment and improvement of the CGCS. Refer to Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Sustainment Management Policy, COMDTINST 5230.72 (series) for additional information.

B. Communication Requirements. (Excluding Enterprise Data Network and Telephony Services). The Assistant Commandant for Capability, Commandant (CG-7), oversees the CG's operational requirements management process. The Office of Command, Control, Communications, Computer, Cyber, and Intelligence (C5I) Capabilities, Commandant (CG-761) promulgates operational communication requirements. The Office of Command, Control, Communications, Computer, Cyber, and Intelligence (C5I) Program Management, Commandant (CG-68) promulgates functional communications requirements. All new communication requests are subject to the C5I Requirements Management Process managed by Commandant (CG-761). Final approval of requirements is coordinated jointly by Command (CG-68) and Commandant (CG-761). Upon approval of a requirement the Communications Portfolio will submit a recommendation to the Command, Control, Communications, Computer, Cyber, and Intelligence Resource Council for funding approval.

   1. Systems installed outside the C5I Requirements Management Process are subject to removal.
   2. Refer to the following documents prior to initiating a new request:
      a. Requirements Generation and Management Process, Pub 7-0;
      b. Cutter, boat, or aircraft, C4ISR Operational Requirements Document (ORD), for major acquisitions; and,
      c. C5I Requirements Management Process Guide.

C. Authority to Operate (ATO) and Authority to Connect (ATC). All systems connected to CGOne and SIPRnet must have an approved ATO and an approved ATC by CGCYBER. Commandant (CG-26) approved ATO and ATC are required for connection to JWICS. Specific policy on how to obtain an ATO and ATC is found in the U.S. Coast Guard Cybersecurity Manual, COMDTINST M5500.13 (series).

D. Radio Systems Procurement.

   1. Maritime Mobile Radio (MMR) and Ancillary Equipment Procurement. Units with a need for any mobile, portable, or fixed tactical communication radios and/or any ancillary radio equipment, to include key variable loaders (KVL), will adhere to the following policies:
      a. The C5ISC is the only authorized procurement authority for MMR and ancillary equipment. The only exception for this is vessel and aircraft acquisitions executed by the Director of Acquisition Programs, Commandant (CG-93);

b. All newly procured or acquired tactical VHF and UHF radios must be dual or multi-band enabled. This includes radio procurements for all acquisition projects, legacy cutters, and boats requiring upgrades;

c. CG use of Family Radio Services (FRS), General Mobile Radio Services (GMRS), citizens band (CB), and MURS (Multi Use Radio Service) are not authorized for procurement per FCC regulations and all requests for approval or waiver will be denied; and,

d. Maritime Mobile Service Identity (MMSI) Maintenance. Commandant (CG-672) must assign and manage CG MMSIs. Newly established CG shore and afloat units without an MMSI can request one from Commandant (CG-672). Acquisition activities must coordinate with Commandant (CG-672) to obtain a MMSI for new equipment. For replacement equipment, the MMSI must be transferred to the replacement equipment as it is installed by the regional Base C5I department/Electronic Systems Support Detachment (ESD) or other installing activity.

2. Land Mobile Radio (LMR) Systems. The procurement of LMR systems is not authorized unless the CG unit is requested and authorized in writing by a state or local government agency for the purpose of interoperability. The procurement and support of LMR equipment needed to meet these unique regional or local interoperability requirements must be a unit expense. See Chapter 9, Communications Plans and Exercises, for amplifying information on establishing local interoperability agreements.

   a. Programmatic funding is not available for expanding regional communications interoperability with local government agencies.

   b. Units must advise their servicing Base C5I Department of any planned procurement and installations.

3. Cryptographic Equipment. Units with an operational requirement for cryptographic equipment must notify Commandant (CG-62).

4. Satellite Communication Acquisitions.

   a. Iridium Satellite Phones. C5ISC is the sole provisioning agent for Enhanced Mobile Satellite Services (EMSS) Iridium satellite phones on the DOD contract, including obtaining secure capabilities.

      (1) The procurement of services from this contract must be approved by Area or District commanders and Commandant (CG-68).

      (2) DOD contract services can be procured using unit funds, but units must order services through C5ISC.

      (3) Units must follow specific Area procedures provided on the C5ISC Supported System CG Portal page for the repair or acquisition of new or replacement equipment.

   b. Military Satellite Communication (MILSATCOM) Equipment. Units must follow C5I Requirements Management Process for the procurement of new MILSATCOM equipment.

E. Enterprise Data Network, Telephony, and Commercial Services Acquisition. The following section provides information on the procurement of network, telephone, and commercial services.

1. General. For all telephony voice, data, video and peripheral equipment products and services (less TS/SCI systems), units should contact C5ISC via their Base C5I Department for assistance in conducting on-site surveys for requirement analysis, planning, designing, engineering, configuration and preparing the Statement-of-Work (SOW).
   a. Acquisition and installation requires thorough planning for efficient and effective application of approved C5I technology to ensure systems are properly deployed, operated, and supported. Therefore, only the C5ISC is authorized to procure or approve procurement of and install telephony, PBX and video equipment. This includes voice mail (VM), automatic call distribution (ACD) and video teleconference (VTC) equipment.
   b. The CG must only acquire C5I telephony products that are C5ISC approved and fully interoperable with existing systems.
   c. Base C5I Department must forward the request for review and approval via Commandant (CG-68) and C5ISC. Specific detailed guidance for Base C5IT Departments is located on the Commandant (CG-68) CG Portal page.
   d. Voice services ordered must be capable of providing caller identification (caller ID) and automated number identification (ANI) services as standard features.
   e. All equipment ordered must be new. No re-manufactured power supplies, circuit cards, CPUs, hardware, electronic or other installation parts are authorized with system outfitting, for provided spare parts, or for parts provided to perform warranty repairs unless prior approval is obtained from the C5ISC.
   f. All systems proposed for each order must be of the same manufacturer.
   g. Requests for video teleconferencing products and services must be routed to (C5ISC-UCPL) by submitting a CGFIXIT help desk request for New VTC Service. Requests for secure VTC systems and services must initially be routed through the local command Information System Security Officer (ISSO) and KMI manager for approval of additional encryption devices to be added to the secure inventory.
   h. All video conferencing services and components must be DISA Joint Interoperability Test Command (JITC) certified and listed on the DISA Authorized Equipment List (AEL), and be fully interoperable with existing systems.
   i. The unit requesting video teleconferencing services, is responsible for providing all necessary funding for the procurement, installation, maintenance, and support of all requested video conferencing systems, as well as the necessary communication circuits and/or infrastructure required for use.

j. The C5ISC in coordination with Product Line Managers (PLMs) must prepare an annual budget based on a requirements analysis (looking forward at least 3 years), a priority list of CG facilities that require replacements, upgrades, expansions or maintenance, and forward the report and request to Enterprise Infrastructure Portfolio Working Group Lead, for review, approval, and funding during the resource proposal (RP) or other budget planning process.

2. Enterprise Data Network Service Requests. DODIN, NIPR, and SIPR gateway circuits currently exist at the C5ISC. C5I Product lines are establishing JRSS/DISN MPLS at C5ISC that will provide all Coast Guard users a gateway into the DODIN. Area and District Commanders, unit commanding officers, and directorates/special staff divisions at CG headquarters must:

   a. Submit requests for enterprise data network services by CG memorandum to C5ISC thru their chain-of-command. See Reference (a) for a list of information required to be included in the request.

   b. JWICS. Units must submit request for JWICS installation, de-installation, and support to Commandant (CG-26).

3. Authorized Procurement Personnel. The following section describes personnel authorized to procure network, telephony, and commercial services.

   a. Coast Guard (CG) Telecommunication Certification Office (TCO). The CG designated TCO, must comply with all DISA/DITCO policies and procedures for requesting communication services or facilities. For TCO codes, refer to Reference (a).

   b. Designated Agency Representatives (DAR). DARs are field representatives assigned to the regional Base C5I department and other designated commands authorized and trained as Ordering Officials to order communication services. DAR authority is limited and managed by the DAR administrator at the C5ISC.

      (1) CG DARs are the only authorized agents allowed to place orders for communication circuits and services (excluding cellular phones) from approved sources and must use the most current policy and practices promulgated by the C5ISC.

      (2) DARs must be designated in writing by the DAR administrator and certified as contracting officer's representatives.

4. Federal Telephone Services (FTS) Contracts. FTS contracts provide the CG with enterprise and local unclassified communication services to include, but not limited to, long distance switched and dedicated voice service, WAN (e.g., CGOne), RESCUE 21, audio/video conference calling, Internet gateways, toll free service, Large Capacity Disaster Recovery Network, fixed satellite services, enterprise product lines, and various other data and voice services to meet CG mission and unit requirements. The following section outlines policy for FTS services.

   a. Units requiring FTS services must coordinate requests with the servicing DAR.

   b. Enterprise services are circuits and services identified by Commandant (CG-68) and supported through enterprise funding. These circuits include, but are not limited to, CGOne, RESCUE 21, NDRS, CSN, switched long distance service, and long distance dedicated PBX trunks. Units requesting additions, moves and/or changes to enterprise services must route a service request, in writing, to the C51 SC via their local servicing DAR and provide associated funding to support the new requirement(s).

c. Units that require non-enterprise or local service must route a service request, in writing, to the local servicing DAR. The primary source of funding for unit-specific requirements for communication circuits and services provided by local exchange carriers or federal communication contracts must be direct billing to account strings. If direct billing does not meet accounting system circumstances then centralized billing can be used with associated funding to support the initial requirement(s) through the end of the fiscal year supplied by the requesting unit. When centralized billing is necessary, service charges are billed back to the unit annually. Non-enterprise or local services include, but are not limited to:

(1) Voice Service (e.g. toll-free service, audio and video teleconferencing, local dial tone, Centrex service, voicemail);

(2) Commercial Direct-Inward-Dial PBX trunks and numbers;

(3) IP-based services (e.g. IP service, VoIP, digital subscriber line (DSL));

(4) Video transmission service (Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI)/Primary Rate Interface (PRI) wide-band video transmission service (full motion) switched video);

(5) Switched data services (e.g., ISDN, Switched 56kb); and,

(6) Packet Switched Services (e.g., point-to-point dedicated access or dial-up access).

5. Microwave Point-to-Point Wireless Services. Units determining a need for microwave point-to point wireless services must adhere to the following policies:

a. The C5ISC is the only authorized procurement authority for microwave point-to-point wireless services; and,

b. Once new microwave service is validated and approved, microwave wireless transmission services must be funded by the local unit and their regional communications manager.

6. Cellular Telephones and Portable Electronic Devices (PEDs) Equipment/Services. Service wide management of all CG owned mobile cellular wireless devices and services has transitioned to the Cellular Wireless Managed Services (CWMS) program. Therefore, unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements are no longer permitted to procure cellular equipment and usage services directly from any vendor. CWMS uses the provision and services of a DHS mandatory use blanket purchase agreement administered by a telecommunications expense management firm. This agreement covers CG wide cellular wireless contracts and services including all smart phones, standard cellphones, mobile hotspots (MiFi's), and tablets with cellular connection. In order to effectively manage this program:

a. The C5ISC must appoint a senior management representative to administer the program on behalf of the CG.

b. Each unit must assign a collateral duty unit Cellular Resource Manager (CRM).

c. Unit CRMs must:

(1) Ensure the accurate assignment of devices to authorized members;

(2) Manage international service and other special service needs;

(3) Order new devices and services as required;

(4) Order replacement devices; and,

(5) Validate authorized device usage to ensure compliance with Reference (k) and other processes as required.

d. The following applies to all cellular telephones and PEDS:

(1) Unconstrained use can result in excessive airtime costs. Units must closely monitor cellular telephone and PED usage and must establish local policies and procedures (e.g., IT Configuration Control Board) for effective management and oversight;

(2) Cellular systems do not provide COMSEC unless a global security module (GSM) for mobile communication security is used. Requests for procurement of secure cellular telephone modules must be forwarded to Commandant (CG-68) via the chain of command; and,

(3) Only government purchased cellular phones and PEDs are authorized to load CG portable Email and other CG owned or licensed software.

7. Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS). DHS OEC offers priority communication services to enhance the ability of critical national security and emergency preparedness personnel to communicate during disasters. GETS and WPS is a service for government provided land lines and cellular phones only.

a. GETS provides authorized personnel priority calling on the public telephone network during an emergency or crisis situation when the probability of completing a call is reduced due to excessive call volumes; and,

b. WPS provides the same priority for cellular networks. Note: See Reference (a) for GETS and WPS procedures.

8. Non-Appropriated Funds Instrumentalities (NAFI). Appropriated funded telephone service may be provided to NAFI programs. Use of these services is restricted to command and control purposes, including safety and security, and other official CG business and programs per the Coast Guard Non-appropriated Fund Instrumentalities (NAFI) Manual, COMDTINST M7010.5 (series) and the Coast Guard Morale, Well-Being, and Recreation Manual, COMDTINST M1710.13 (series). Procuring services for other NAFI business activities is limited to services that can be established to directly-bill to the facility or through reimbursement if direct billing is not practical. The following section outlines additional NAFI policy.

a. Government funded local telephone services are not authorized for credit unions on CG property, but may be provided on a reimbursable basis.

b. Local telephone services paid with appropriated funds are not authorized for installation in residences. However, government owned/leased facilities are exempt from this restriction. Appropriated funds may also be used for the installation and maintenance of a STE in CG flag officer residences in support of the Maritime Defense Zone mission and national security. Commandant (CG-6) must approve this service with concurrence from DHS.

CHAPTER 5 OPERATIONAL COMMUNICATIONS

A. General. CGCS networks and systems are operated as per DOD and CG CIO policies. All units must follow the policies and forms of communication prescribed in this Manual using tactics, techniques, and procedures per Reference (a). All pertinent ACPs, Joint Army, Navy, Air Force Publications (JANAP), CG LANTAREA and CG PACAREA instructions, International Civil Aviation Organization (ICAO), Federal Aviation Administration (FAA) publications, FCC policy and ITU policies, treaties and agreements apply.

B. Communications Officer/Communications Supervisor. A communications officer or communications supervisor must be designated in writing at all units that maintain any type of communication watch. The communications officer or communications supervisor must be responsible for the conduct of proper communication for the command. Communications officer or communications supervisor duties must be incorporated into Annex K to Area OPLAN, District supplement, and unit standard operating procedures (SOP), as applicable. Further information on the duties and responsibilities of the communications officer is found in Reference (i). Information on the duties and responsibilities of the communications supervisor is found in Reference (j).

C. MINIMIZE. MINIMIZE is a set operational communications condition wherein normal messaging, radio, and telephone traffic is drastically reduced so that information associated with an actual or simulated emergency is not delayed.

1. Authorization. Authorization to implement MINIMIZE must be as follows:
    a. Normally, the unified commands issue the MINIMIZE order;
    b. Designated commanders may request other commanders or friendly foreign countries to impose MINIMIZE;
    c. Commanders may request the Chairman, Joint Chiefs of Staff (CJCS) impose MINIMIZE on users in other areas that originate traffic destined for addresses in the area under MINIMIZE;
    d. The commanders or chiefs of other agencies may be requested to impose MINIMIZE on all users required to communicate with activities in the MINIMIZE area, or whose communication services pass through the communication facilities of the area under MINIMIZE; and,
    e. All Area and District Commanders and unit commanding officers may impose MINIMIZE within their AOR unless specifically denied by higher authority. When MINIMIZE is imposed upon worldwide networks, Area and District Commanders may authorize relaxed conditions of MINIMIZE over networks or circuits entirely within their control.
2. Implementation.
    a. The CJCS or a commander of a unified or specified command can impose MINIMIZE upon all or part of their areas of command responsibility by general record message. These general record messages must automatically apply to CG forces in the area specified.
    b. CG record messages implementing MINIMIZE must include the applicable operational commander, District and Area Commander, and Commandant as addressees. Unless otherwise stated in the record message, the MINIMIZE is effective for all communication circuits and or Networks.
    c. Procedures to request CG-wide MINIMIZE are in Reference (a).

3. Enforcement. Enforcing MINIMIZE is a command responsibility, and is imposed upon users, not information systems and communication networks. The commanding officer must not permit release of non-exempt record messages when MINIMIZE is imposed on the record messaging system.
4. Exemptions. Certain types of record messages are exempted from MINIMIZE to preclude interruption of important operations. Types of record messages exempted from MINIMIZE are:
   a. Directly related to a particular mission accomplishment or operation;
   b. Safety of life;
   c. Critical intelligence;
   d. Perishable weather/navigation information;
   e. Status information or instructions pertaining to the communication system affected by MINIMIZE;
   f. Casualty reports (CASREP);
   g. Aircraft and fleet unit movements;
   h. Continuing research and development programs vital to national interest; and,
   i. Serious illness, accident, or death involving CG or DOD personnel and members of their immediate families.
5. Record Messages. Commands must specifically designate users with record message release privileges during periods of MINIMIZE. Per Reference (a), CG record messages meeting the criteria for release during MINIMIZE must include the following as the last line of the text: "Released by (name and rank/grade)."
6. River City. Afloat commands should become familiar with the River City procedures. River City is a data management technique that originated with U.S. Naval operations, and adopted by USCG Cutters initially as part of Joint PATFORSWA Operations. It is a process to support an On-Demand capability restricting activity by user and/or application by leveraging policies or add-on software. Units must contact the CSD for more information about implementation.

D. Telephone Management.

1. Telephone Management Programs. The Telephone Management Program must be administered by the C5ISC. Local programs must be implemented and administered by Base C5I departments. Local programs must ensure the following:
   a. Personnel are aware of the proper and effective use of telephone services to include policies on personal use as detailed in section D.2. of this Chapter;
   b. CG DARs are familiar with and comply with applicable Federal Management Regulations and Federal Acquisition Regulations for procuring and managing telephone services. DARs must check all invoices or accounts under their ownership to certify the accuracy of the inventory and associated charges. The schedule for these checks must be continuous throughout the year, but must be completed by the end of the third quarter of each fiscal year. All unnecessary equipment and features must be removed;

c. Where practical, consolidated or common user systems must be used to provide service to multiple CG units; and software blocks to unapproved area codes (e.g., 900) must be implemented whenever possible on CG owned/leased telephone systems.

2. Telephony Policy for Personal Use of Government Office Equipment. Policies regarding authorized, inappropriate, and prohibited uses of CG office equipment are outlined in Reference (k).

   a. Long Distance Data Use. Long distance telephone networks must not be used for data transmissions (except for use of secure and non-secure facsimile (FAX). Requests for waivers from this policy must be submitted in writing with supporting rationale to Commandant (CG-68).

   b. Requirements for all calls. The following policy pertains to all personal local and long distance calls:

      (1) Call must not adversely affect an individual's or other's performance of official duties; and,

      (2) Call must be of minimum duration and frequency.

   c. Local calls (within the local commuting area). Telephone companies charge the CG and other government activities at the business rate. Business rates do not provide unlimited local calls in the basic service plan, so all local calls are billed. CG employees are authorized to place the following types of local calls within the local commuting area using government telephones:

      (1) Calls to notify the family doctor when an employee is injured on the job;

      (2) Calls to arrange transportation or childcare when an employee is required to work unscheduled overtime;

      (3) Brief calls to speak to spouse or minor children, or those responsible for child care;

      (4) Calls that can only be made during working hours (e.g., local government agency, physician);

      (5) Calls to arrange for emergency repair to a residence or vehicle; and,

      (6) Calls certified as official in advance by the employee's supervisor.

   d. Long Distance Calls. Long distance calls not related to assigned duties that must be made during normal working hours must be:

      (1) Charged to an individual's home or other non-government phone number;

      (2) Made to a toll-free number;

      (3) Charged to a personal credit card; or,

      (4) Collect.

   e. CG Auxiliary Use. DSN services are not authorized for CG Auxiliary members.

   f. Toll-free Service. Toll-free telephone service (800/866/888/877/855) that allows the public to make a long distance call at government expense must be approved by the C5ISC. Units requesting toll-free service are responsible for charges incurred by the service.

3. Private Branch Exchange (PBX) System Security. Call forwarding, PBX, Voice Mail (VM) , auto attendant, and Automatic Call Distributor (ACD) Class-of-Service (COS) are subject to serious threats by hackers. Threats include, but are not limited to, theft of proprietary/personal and/or confidential information, use of unit's dial-tone to place telephone calls all over the world at U.S. Government expense (toll fraud), and loss of outward dial capability (all trunks busy) affecting communications during critical events thereby rendering these communication services ineffective.
4. Call Forwarding. Call forwarding of any government phone to a personal cell phone or landline is prohibited. Call forwarding to a government owned device (cellular/smart phone) is authorized for commands to conduct official CG business (e.g., recall, designated duty personnel, help desk, travel, and continuity of operations (COOP).
    a. Local Security Measures. For all units within their respective AOR, Base C4IT departments must verify and/or take the following actions to ensure that PBX, VM, auto attendant and ACD Systems are protected from unauthorized access:
        (1) Ensure that PBX systems cannot provide outside dial-tone to an incoming caller and allow that caller to dial their desired number;
        (2) Disable direct inward system access;
        (3) Ensure system access codes/passwords are restricted and have been changed from the default password;
        (4) VM passwords must be changed every 90 days;
        (5) Ensure incoming remote maintenance access cannot be forwarded to outside trunks; and,
        (6) Ensure call detail recording (CDR) monitoring system records are analyzed monthly for security breaches, fraud, waste and abuse.
    b. Hacking Unauthorized Access Prevention. PBX, VM, auto attendant and ACD procedures must be implemented to prevent criminals from gaining access into systems. These procedures also help to limit fraud, waste, and abuse:
        (1) Ensure that all applicable PBX administrators receive instructions and training on these Call Forward techniques;
        (2) In VM Systems, Dial-by-Name is not authorized per Reference (l). Electronic directories that request the spelling of the last name of the person you would like to contact must be disabled. Contact the equipment vendor for specific instructions if necessary; and,
        (3) Caller ID must be provided on all PBX telephones, local exchange carrier (LEC) and General Services Administration (GSA) Federal Telephone System (FTS) trunks.
5. Local Telephone Directory Listing. To minimize delay in reporting distress cases and other emergencies, clear and precise unit directory listings with correct telephone numbers must be arranged with local telephone companies. Units must ensure their local telephone company's directory list managers provide work with local telephone companies to keep the listings current. In addition:
    a. Directories must include Area, District, and Sector Command Centers in the AOR; and,

b. Whenever possible, list emergency numbers under "Emergency Calls," in the front section of the directory, and under the "U.S. Government" heading in the directory's body. For standardization, list command center numbers under the "Coast Guard Search and Rescue Emergencies" heading.

6. Emergency Telephone Number 911. The emergency telephone number 911 is designated nationally for public use in reporting emergencies and requesting emergency services. The responsibility for establishing a 911 program resides with local governments. The following outlines additional policy for 911 participation.

   a. CG participation in 911 is encouraged where the local program can effectively satisfy communication requirements with the public.

   b. District Commanders, after evaluation of local programs, must determine their own levels of participation and funding requirements. See Chapter 9, paragraph F., Interoperability Planning, for information on how to establish formal agreements with partnering agencies.

7. Uninterrupted Power Supplies (UPS). Telephony and peripheral systems must be backed up by UPS.

8. Telecommunications Service Priority (TSP) Services and Database. TSP is the regulatory, administrative, and operational system authorizing and providing for priority treatment (i.e., provisioning and restoration) of national security and emergency preparedness communication services.

   a. Commandant (CG-68) is the TSP program manager for the CG.

   b. Management and ordering functions must be per policy and practices promulgated by the C5ISC.

   c. The C5ISC must maintain the DHS OEC TSP database for all communication circuits.

E. Audio/Video Teleconferencing. Audio/video conferencing leaders must actively monitor the conference to ensure only authorized participants are on the line. Reference (a) contains further procedures for safeguarding audio and video conferences.

1. CGOne is not designed to support live streaming video for large number of users. Real-time video streaming requests must be prearranged and authorized by Commandant (CG-68) via the Area C5I division (LANT-6/PAC-6).

2. To minimize impact on CGOne, commands are encouraged to use dayrooms/conference rooms for maximum viewing of mandatory or CG-wide interest videos. This does not prevent users at individual workstations from viewing a video.

3. The timing of video release is critical to CGOne performance. When possible, videos must not be published on Mondays or Fridays to minimize the impact on personnel telecommuting.

4. The standard video resolution for CG-wide videos must be 640 x 480 pixels. Videos requiring a higher resolution for CG-wide viewing must be approved by the C51SC prior to publishing.

F. Facsimile (FAX). FAX is used for any level of correspondence between CG commands where timely service is required. However, FAX does not provide users with any level of security unless a secure FAX configuration is used.

1. As specified in DHS Management Directive Number 11042, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, “Unless otherwise restricted by the originator, FOUO (For Official Use Only) information may be sent via non-secure FAX.” However, the use of a secure facsimile machine is highly encouraged. Where a non-secure FAX is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end. The holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator. If specific guidance on FAX is needed, individual commands must check with their District communications office or Area C5I office.
2. Secure FAX. The term "secure facsimile" refers to a combination of the secure telephone equipment (STE) and a FAX machine meeting the standards outlined in Reference (m).
    a. Minimum security requirements for the handling and control of STE terminal equipment and associated cryptographic keying material (keymat) are found in Reference (n); and,
    b. Each command must ensure that adequate physical security and classified material control procedures are established to account for and safeguard the secure facsimile terminal equipment and classified documents sent or received via secure FAX. Specific guidance is found in Reference (g).

G. Radio Code Plugs. This section provides policy for CG standard mobile, portable, and aviation tactical communications radios and information regarding code plug and Remote Programming Window (RPWIN) support.

1. Commandant (CG-68), is the only entity authorized to approve changes to standard code plugs. C5ISC-ESD-ASB provides enterprise management of standard code plugs to ensure all platforms throughout the CG have the same baseline frequency plan programmed into their mobile and handheld radios. All units must maintain the standard code plugs in their mobile and portable VHF and UHF radios.
2. Area communication divisions and District communication offices, with the support of their regional spectrum manager, must validate and add local District/Sector frequency requirements to the Area or District frequency plan and code plug/RPWIN, referred to as zones of convenience. Area modified code plugs are best suited for Area cutters and Deployable Special Forces units.
3. A copy of the modified code plug/RPWIN must be provided to Commandant (CG-68). The modified files must be made available on the C5ISC portal and Area/District portal sites.
4. Base C5IT department must be responsible for installing modified code plug and RPWIN files. Modified code plug and RPWIN files must be obtained from the District communications staff.
5. Aviation assets do not require zones of convenience modifications, just the addition of District unique requirements to the C5ISC code plug and remote programming windows RPWIN files.

6. Aviation maintenance personnel must be responsible for the loading of appropriate code plugs and RPWIN files into aviation radios and for making all permitted modifications to unassigned presets within the first 25 present positions of the RPWIN build for local air traffic control unique additions. The completed RPWIN file must be provided to the regional spectrum manager for publication.

H. Use of Public Maritime Channels Maritime Mobile Bands. Units and other mobile assets not capable of digital communications and units communicating with platforms without digital communications capabilities are authorized use of the following maritime channels in analog clear or unprotected mode until the requirement for analog tactical communications no longer exists. The use of these public maritime channels should only be used as a last resort for tactical comms. The following channels are authorized for use when communicating with the maritime public or when no other method of communication is suitable:

1. VHF-FM Channel 16 (156.800 MHz) - International calling and distress frequency
2. VHF-FM Channel 21A (157.050 MHz) - Maritime/air/ground SAR working frequency
3. VHF-FM Channel 23A (157.150 MHz) - Maritime/air/ground SAR working frequency
4. VHF-FM Channel 81A (157.075 MHz) - Interagency response channel for pollution response operations. Use only when no other listed channel is available.
5. VHF-FM Channel 83A (157.175 MHz) - Also used for Mariner Radio Activated Sound Signal (MRASS) device.
6. Shore station use of VHF-FM Channel 13 (156.650 MHz) and VHF-FM Channel 67 (156.375 MHz) is authorized only for the transmission of navigation related information.

I. Radio Checks with Mariners.

1. It is not uncommon to receive a radio check request from a mariner on VHF-FM Channel 16 (156.800 MHz). Mariners must be encouraged to conduct radio checks with other mariners. The only response to a radio check on this channel must be "(vessel name), roger out".
2. The RESCUE 21 system provides an automated response to test calls on VHF-FM Channel 70 (156.525 MHz) for VHF DSC radios equipped with the Test Call feature. Test transmissions should be made to the U.S. Coast Guard MMSI 003669999 to receive an automated VHF DSC test response. Mariners must use the "Test Call" category of their radio because "Individual" category calls to this address will not receive an automated response. For older radios not having a test call capability, testing can only be performed by using a routine individual call to their Maritime Mobile Service Identity (MMSI). Under no circumstances must a DSC Distress Alert be sent to test your radio.

J. Automatic Identification System (AIS).

1. AIS is a ship-to-ship collision avoidance system that allows for communication of position, speed, and other ship data via a VHF virtual data link (VDL) network. Mariners worldwide use AIS to ensure safety at sea
2. Only unclassified information must be transmitted on AIS. CG commands must use an encrypted message to send FOUO or SBU information.

3. AIS may be used to augment the Global Maritime Distress and Safety System (GMDSS) and provide the added benefit of visual radar or chart displays in addition to audio transmission by other AIS users within VHF radio range. For further guidance, USCG Safety Alert 5-10 is located on the NAVCEN website (https://www.navcen.uscg.gov) or refer to International Maritime Organization's Circular 46, Use of AIS Safety-Related Messaging in Distress Situations.
4. Nationwide Automatic Identification System (NAIS) is a nationwide network of land-based VHF receivers and transmitters designed to increase Maritime Domain Awareness (MDA) in U.S. coastal and territorial waters. Numerous NAIS sites along the coast "listen" to transmitted maritime AIS activity; this data is then consolidated and disseminated to the Coast Guard and other government agencies. For more information, please visit https://www.navcen.uscg.gov.

K. Iridium Satellite Phones. Iridium satellite phones are a component of the Defense Information Systems Network (DISN) and are the only commercial satellite phone that meets all DOD requirements for secure handheld mobile satellite service.

1. Iridium satellite phones provide no communication security unless the secure module is used with an activated DOD subscriber identity module (SIM) on a securable, tamper-sealed handset.
2. Iridium satellite phones are portable electronic devices subject to policies and procedures outlined in Reference (n).
3. Iridium Enhanced Mobile Satellite Services phones become classified when connected to the Iridium security module (ISM) and the user personal identification number (PIN) is entered allowing secure communications.
4. The user PIN must be stored in a safe place and is unclassified (FOUO) when not stored with the associate ISM.
5. The ISM is a controlled cryptographic item (CCI) and must be stored and shipped per Reference (n).
6. Loss of the ISM with or without the phone is a reportable physical incident requiring action per Reference (n).
7. CG Iridium phones obtain airtime services in one of two ways: either through the Defense Information Systems Agency (DISA) or a commercial provider. Reference (a) contains procedures for identifying airtime service type for Iridium satellite phones. Commands must identify which airtime service the unit Iridium satellite phone uses to prevent the misuse of Iridium equipment.
8. Use of DISA Iridium satellite phones (non-commercial) for morale calls is authorized per Reference (n) at the commanding officer's discretion. Defense Information Systems Network Mobile Satellite Systems is procured through DISA and consists of a monthly flat rate per phone with unlimited use.
9. Iridium phones on commercial service plans are designated for contingency operations. These Iridium phones may be used for other operations requiring only clear (non-secure) communications. Funding for service plan costs must be taken into consideration. Morale calls on commercial accounts are not authorized.

10. Unless permanent shipboard mounts are installed per an approved Time Compliance Technical Order (TCTO), Iridium satellite phones must be used with the handset only. Temporary magnetic mount of external antennas is authorized and may be used as deemed necessary by the command.
11. Communication checks on Iridium satellite phones used less than twice a month must be conducted monthly to ensure the equipment is ready for operations. Phones capable of secure communication must be tested in both clear and secure modes.
12. Commands must maintain a unit inventory containing the Iridium phone number, Iridium phone model number, SIM number, and the International Mobile Equipment Identity (IMEI) number.
13. Units must contact LANT/PAC-6, or the C5I Product Line Iridium phone manager for further guidance on tamper seals and/or ISMs.

L. Military Satellite Communication (MILSATCOM).

1. Department of Defense (DOD) Satellite Database. Commandant (CG-68) must manage the CG MILSATCOM mission data entries in the DOD satellite database. This includes annual review/update, removal, and submission of new entries through NORTHCOM for review by the Joint SATCOM Panel.
2. System Configuration. All MILSATCOM system configuration changes at shore or afloat units must be conducted per Reference (o). For guidance on MILSATCOM system configuration changes for aviation assets, contact the Office Aeronautical Engineering, Commandant (CG-41).
3. Terminal Base Address (TBA). The TBA is a unique address assigned to identify each MILSATCOM user (e.g., CGC TAMPA). All MILSATCOM terminals must have a TBA for access to a MILSATCOM Demand Assigned Multiple Access (DAMA) channel. Units that obtain any new or previously owned MILSATCOM systems must submit a TBA request per Reference (o).
4. Satellite Access Requests. Satellite Access Requests. The submission of a satellite access request to Northern Command (NORTHCOM) for all MILSATCOM system access is required per Reference (p). All satellite access requests must be submitted via the Joint Integrated Satellite Communications Tool (JIST).
5. Extremely High Frequency (EHF) Access. Units must submit a satellite access request to the COMMCOM no less than 45 days prior to the start of the mission for all EHF access per Reference (p). COMMCOM will review the request and forward it to NORTHCOM 30 days prior to mission start. For specific guidance, cutters must use the EHF Satellite Access Request Standard Operating Procedure provided by the system support agent. Units requiring status update on their requests must contact COMMCOM. COMMCOM is responsible for facilitating EHF related communication issues between the cutters and servicing EHF facility.
6. MILSATCOM Networks. Networks include:
   a. Satellite high command (SATHICOM) (USN tactical voice);
   b. Joint Interagency Task Force (JIATF) air;
   c. JIATF surface (JIATF South tactical voice);

d. Common User Digital Information Exchange Subsystem (CUDIXS), a transmit and receive system used for tactical record messages with up to a Top Secret classification level;

e. Fleet Satellite Broadcast Subsystem, a USN receive only record message system authorized up to the Top Secret classification level but currently used for the classification level Secret;

f. Colombian Navy (COLNAV). COLNAV is the JIATF Columbian Navy circuit;

g. Homeland Security Network (HLS Net). DAMA and Non-DAMA tactical voice nets with COMMCOM serving as Net Control Station (NECOS). HLS is an open net, therefore, no request to relinquish the net is required; and,

h. DISA application PDA-184. Used for imagery transfer and chat. DAMA and Non-DAMA tactical data network with Maritime Intelligence Fusion Center Atlantic or Pacific (MIFC LANT/PAC) serving as NECOS for their respective networks.

M. Lost Communications.

1. Shore units that lose communication with a CG vessel for which they have the guard must attempt to reestablish communication directly with the vessel or through another station. If an underway vessel fails to check in on either the primary or secondary frequency within 10 minutes of its communication schedule, OPCON takes all necessary action to reestablish communications, either directly or through another unit. Reference (a) contains sample lost communication procedures for vessels.

   a. If no communication is established, lost communication notifications must be made. When communication is reestablished with the vessel, all alerted units must be notified;

   b. Area and District Commanders may publish additional policy for alert procedures in lost communication situations.

2. Shore units that lose communication with an aircraft for which they have the guard must initiate the necessary actions to re-establish communication with the aircraft either directly or through another unit. If the aircraft commander fails to check in on the primary or secondary frequencies within 5 minutes of the communication schedule, the guarding unit must initiate an alert. Reference (a) contains sample lost communication procedures for aircraft.

   a. Area and District Commanders can publish additional policy for alert procedures in lost communication situations. The aircraft's parent command must be notified first, followed by the cognizant District CC;

   b. When communication is reestablished with the aircraft, all alerted units must be notified.

N. CG Shore Unit Radio Frequency Guard Requirements. See Chapter 11 for CG SAR communications and DSC response policies.

1. CG Sectors equipped with RESCUE 21 must guard VHF-FM Channel 70 (156.525 MHz). DSC test calls received via VHF are automatically answered by the RESCUE 21 system and do not require operator intervention.

2. VHF-FM Channel 70 is non voice. DSC only.

3. Equipped CG shore stations must maintain a continuous watch on VHF-FM Channel 70 DSC only. (156.525 MHz).

4. Equipped CG Sectors must maintain an uninterrupted guard on VHF-FM Channel 16 (156.800 MHz).
5. Additional specific guard requirements for operations must be specified in Annex K to Area OPLAN, District Annex K or Supplement, and Sector Communication Plans or Standard Operating Procedures (SOP) as appropriate. See Chapter 9, Communication Plans and Exercises.

O. Area, District, and Sector Command Centers (SCC). SCCs function as the focal point for control of CG forces and are staffed by personnel with the skills and expertise to ensure safe and effective operations. SCC watchstanders require direct communication capabilities with DOD organizations, federal agencies including DHS, state, local, and tribal officials, and the general public. Operational commanders specify requirements for communication facilities located in the SCC.

1. All operational telephone circuits must be terminated in the SCC.
2. SCC watchstanders must have the ability to communicate secure, protected, and unclassified voice communication capabilities with on-scene commanders.
3. Operational telephone and voice radio circuits must be continuously monitored by means of electronic recording devices.

P. Rescue 21.

1. Information that is classified or SBU must not be transmitted on the RESCUE 21 interconnected intercom because an open microphone on the receiving end could result in compromise;
2. The RESCUE 21 physical system configuration must not be adjusted by Sector personnel. Configuration changes to RESCUE 21 are only authorized by the C5ISC COMM-PL Manager through a formal configuration control board process and must be implemented via Time Compliance Technical Orders (TCTO);
3. Sector Commanders must designate a minimum of two personnel as local RESCUE 21 system supervisors;
4. Systems supervisors are responsible for RESCUE 21 user interface configuration management and locally established user interface configurations within RESCUE 21 for the Sector and boat stations.

Q. Command Center Maritime Public Broadcast Operations.

1. See Chapter 10 for detailed discussion, schedules, and quality control program.
2. Sectors San Juan and Guam are responsible for the Navigational Telex (NAVTEX) broadcast within their AORs. The Communications Command remotely operates all remaining CG NAVTEX broadcasts.

R. Communications Command (COMMCOM). The COMMCOM provides rapid, reliable, secure, nonsecure, or protected, and interoperable communications for CG operational commanders, other government agencies, and the maritime public.

1. The COMMCOM remotely operates a geographically distributed MF and HF infrastructure with unmanned radio facilities with the exception of a communications detachment (COMMDET) located in Kodiak, Alaska. Figure 7 lists each communication facility and the associated call sign.

COMMCOM FACILITIES	
COMMCOM Chesapeake (NMN)	RCF Pt Reyes/San Francisco (NMC)
COMMDET Kodiak (NOJ)	RCF Honolulu (NMO)
RCF Boston (NMF)	RCF Charleston (NME) – NAVTEX*
RCF Miami (NMA)	RCF Astoria (NMW) – NAVTEX*
RCF New Orleans (NMG)	RCF Cambria (NMQ) – NAVTEX*

Figure 7 - COMMCOM Communication Facilities and Associated Call Signs
*NAVTEX (Navigational Telex) Broadcast facility only

2. The following CGCS services are provided by the COMMCOM:
   a. Global Maritime Distress and Safety System (GMDSS). This includes HF DSC and GMDSS voice frequencies. DSC and other GMDSS networks are used for ships to alert coastal stations of distress or other safety-related conditions.
      (1) The COMMCOM must guard the HF DSC frequencies in Figure 8;
      (2) The COMMCOM must maintain continuous radio watch on 4125 kHz as a GMDSS distress and calling frequency in the Seventeenth CG District Area of Responsibility (AOR).
      (3) High Frequency (HF) Automatic Link Establishment (ALE) Networks;
      (4) The DSC system logs test calls on all frequencies, but filters these test calls, except on 4 MHz. The 4 MHz frequency has the Automatic Test Call Acknowledgement (ATCA) function enabled and automatically responds to all tests received. The ATCA is not enabled on the other HF DSC frequencies, but test calls can still be manually answered. ATCA service is available only through the following facilities: COMMCOM, COMMDET Kodiak, RCF New Orleans, RCF Pt. Reyes, RCF Boston, RCF Miami, and RCF Honolulu.
   b. Command and Control (C2) Voice.
      (1) Aircraft HF Flight Following Services. The COMMCOM must provide aircraft safety of flight services using HF Automatic Link Establishment (ALE) through COTHEN. The COMMCOM maintains a detachment at CBP NLECC to assist in COTHEN operation.

(2) Sea, Air, Shore Secure (SASS). The COMMCOM must provide nation-wide SASS capabilities upon request using HF resources at NMN, NMF, NMA, NMG, NMC, and NMO. The list of SASS frequencies can be found in Area OPTASK COMMS.

(3) Military Satellite Communication (MILSATCOM) Networks. The COMMCOM must serve as Net Control Station for the Homeland Security Network (HLS Net).

c. Broadcast Operations. The COMMCOM must broadcast urgent, safety, and scheduled notice to mariners, in addition to, weather and hydrographic information. Broadcast schedules are also provided in Annex C of this Manual and are available to the general public via the following National Weather Service website: https://www.weather.gov/marine/uscg Marine Weather Broadcasts from the USCG.

d. Communications Assist Team (CAT). As directed by the Area Commander, the COMMCOM provides operator-specific assistance, augmentation, and training for baseline operational communication systems, equipment, policies, and procedures. The COMMCOM executes this mission through unit visits to facilitate hands-on experience at the point of action through peer-to-peer exchanges and creates a conduit for candid feedback on operational communications and readiness.

e. Deployable Communications Force (DCF). The COMMCOM delivers communications capabilities throughout the Coast Guard for contingency, surge, and enhanced operations. The COMMCOM maintains highly trained and proficient deployable personnel and a portfolio of assets to include the Mobile Communications Vehicles (MCVs), Enhanced Mobile Incident Command Posts (eMICPs), RESCUE 21 Disaster Recovery Systems (DRS), and a variety of additional deployable communications and computer equipment.

f. CG Auxiliary Communications. The COMMCOM liaisons with the CG Auxiliary for communication support including augmentation, force multiplication, contingency communications support, training, and drills.

g. Call Signs. The COMMCOM establishes CG international HF ALE and SIPRnet call signs.

h. Distress & Safety Statistics. The Marine Information for Safety and Law Enforcement (MISLE) System does not capture distress and distress related safety communications relayed by the COMMCOM. Therefore, the COMMCOM must be responsible for maintaining distress and safety statistics. Statistics must be compiled annually and maintained for a period of five years. Annual calendar year statistics must be provided to the Commandant (CG-672) and the Office of Search and Rescue, Commandant (CG-SAR) within 90 days after the end of the calendar year to enable evaluation of system performance. At a minimum, reports must include:

(1) Numbers of distress alerts received by HF voice, by frequency (e.g., 4125 kHz);

(2) Numbers of other safety and urgency calls received by HF voice (e.g. MEDICO), by frequency, except those initiated by DSC;

(3) Numbers of routine (non-safety related) calls received by HF voice;

(4) Numbers of distress alerts received by DSC, disregarding duplicate calls or relays of calls already received;

(5) Number of DSC distress alerts for which there were follow-up communications by HF voice;

(6) Number of DSC distress alerts for which there were no follow-up communications by HF voice;

(7) Number of DSC distress alerts which did not include a position, or for which a position was incorrect;

(8) Number of DSC distress alerts with an incorrect Maritime Mobile Service Identity (MMSI);

(9) Numbers of safety or urgency calls received by DSC resulting in follow-up voice communications; and

(10) Number of DSC test calls received.

HF DSC Frequency	Associated Voice Frequency
4207.5 kHz	4125 kHz
6312 kHz	6215 kHz
8414.5 kHz	8291 kHz
12577 kHz	12290 kHz
16804.5 kHz	16420 kHz

Figure 8 - HF DSC Frequencies

S. Afloat Units – Cutters and Boats.

1. Vessel Lost Communication. CG vessels losing contact with the guarding shore station must attempt to reestablish communication directly with the shore station or through another station. Reference (a) contains sample lost communication procedures.

   a. Area and District Commanders can publish additional policy for alert procedures for lost communication situations.

   b. Lost communication procedures between a CG vessel and CG aircraft can be found in Shipboard-Helicopter Operational Procedures Manual, COMDTINST M3710.2 (series).

2. Vessel Bridge-to-Bridge Radiotelephone Act. The Vessel Bridge-to-Bridge Radiotelephone Act is applicable on the navigable waters of the U.S. This includes the territorial sea (the waters, 12 nautical miles wide, adjacent to the coast of the U.S. and seaward of the territorial sea baseline), internal waters that are subject to tidal influence, and those waters not subject to tidal influence, but are used or are determined to be capable of being used for substantial interstate or foreign commerce. Regulations in 33 CFR Part 26 outline the purpose of the Act, its associated carriage requirements, designated frequencies, and use and maintenance of radio equipment.

a. Applicability. Commanding officers, officers-in-charge, and conning officers, officer-of-the deck (if actually directing the movement of the CG vessel) must be familiar with the Vessel Bridge-to-Bridge Radiotelephone Act (33 U.S.C. §§ 1201-1208; CG Regulations implementing the act are published in 33 C.F.R. §§ 26.01-26.09). The Vessel Bridge-to-Bridge Radiotelephone Act is applicable on navigable waters of the U.S. inside the boundary lines established in 46 C.F.R. Part 7. The following CG vessels must participate:

(1) Cutters while operating upon the navigable waters of the U.S.; and,

(2) Buoy tenders, aids to navigation boats, or any other CG vessel 26 feet or longer engaged in towing or near a channel or fairway in operations likely to restrict or effect navigation.

b. Interpretation. The Vessel Bridge-to-Bridge Radiotelephone Act (33 U.S.C. § 1204) state bridge-to-bridge radiotelephone is for the "exclusive use of the master or person in charge of the vessel, or the person designated by the master or person in charge to pilot or direct the movement of the vessel." For the CG, this is restricted to the commanding officer, officer-in charge, conning officer, officer-of-the-deck (if actually directing the movement of the CG vessel), coxswain, or licensed pilot and must not be delegated to others. All bridge-to-bridge communications must be conducted in the English language.

(1) All vessels must use VHF-FM Channel 13 (156.650 MHz), except for specific areas in and around the Gulf of Mexico and Mississippi River where VHF-FM Channel 67 (156.375 MHz) is designated, for the exchange or monitoring of navigational information as directed by mission requirements or wherever required to assure safe navigation.

(2) VHF-FM Channel 13 (156.650 MHz) and VHF-FM Channel 67 (156.375 MHz) continuous guard requirements apply. If a CG vessel is operating within a designated vessel traffic service (VTS) area, a separate transmitter/receiver must be used to monitor the VTS frequency.

(3) The bridge-to-bridge radiotelephone frequency must only be used to transmit and confirm the intentions of the CG vessel and any other information necessary for safe navigation.

(4) Inoperable bridge-to-bridge installed radiotelephone(s) is not sufficient cause for nonparticipation. A portable radio can be used as the bridge-to-bridge radiotelephone.

(5) If normal use of the bridge-to-bridge radiotelephone equipment does not demonstrate the equipment is operating properly, units must conduct communication tests prior to getting underway and during each day the CG cutter is navigated. The commanding officer must be notified immediately if the equipment is not in proper operating condition.

(6) The transmitter used on the designated bridge-to-bridge frequency is limited to one watt or less output power for normal operations. If operations require additional output power, it must not exceed 25 watts for ship stations and 10 watts for shore stations.

3. Shipboard Communication Watches. The communication watch is a primary duty assigned to Operations Specialists (OS) afloat. Depending on the size, location, and mission of the CG cutter, the commanding officer is required to establish SOPs to implement communication watch

requirements per the Cutter Organization Manual, COMDTINST M5400.16 (series). Unit communication SOPs must be approved by the commanding officer, and, at a minimum, must be reviewed and updated annually to remain current with unit operational requirements.

a. Cutter Communication Watch Requirements. The billet structure on CG cutters is determined by the personnel allowance list promulgated by the Personnel Allowance Division, Commandant (CG-833). Watch requirements for CG cutters will be per the following guidelines:

(1) Three or more Communications Watchstanders. Maintain a continuous communication watch while underway, at anchor, and when moored where landline or cellular communication are unavailable.

(2) Two or fewer Communications Watchstanders. Watches should be scheduled as dictated by operational conditions per the unit watch quarter and station bill while underway or at anchor, and when moored where landline or cellular communication are unavailable.

b. In port Watch Requirements. To determine the type of in port watch required, the following applies:

(1) When moored at home port or when the cutter is in maintenance and repair ("charlie") status, watches are not required;

(2) When moored away from home port and the cutter has shifted the communication guard to another unit, communication watches should be at the discretion of the operational commander; or,

(3) When moored away from homeport and the cutter has not shifted their communication guard, the units must maintain a continuous communication watch. This includes monitoring record message traffic to meet speed of service requirements.

c. CG Cutters Traveling in Company. CG cutters are permitted to share the communication guard when traveling in company of other vessels/ships.

4. CG Vessel Radio Frequency Guard Requirements.

a. Radio frequency guard requirements for CG vessels are based on laws, regulations, treaties, international agreements, the requirements of the operational commander, the number of OS personnel assigned onboard, and the mission of the cutter.

(1) If a CG vessel is not suitably manned, the operational commander must be notified and corrective action initiated.

(2) CG vessels without an OS assigned are still required to maintain the minimum frequency guards per Figure 9.

b. Under special circumstances, the operational commander can authorize deviations from Figure 9 on a temporary case-by-case basis to meet operational requirements. In granting exceptions, the operational commander should take into consideration that many of the guards listed are required by law, international treaty, or agreement.

c. Voice radio guards must be maintained on the bridge and/or Combat Information Center (CIC). The unit communication plan must ensure all required frequency guards are appropriately allocated between the bridge and CIC.

Vessel Classification	VHF –AM "IAD"/ UHF-AM "MAD" 121.5 MHz 243.0 MHz	VHF-FM Channel 70 (156.525 MHz) (DSC) Note 3	VHF-FM Channel 16 (156.800 MHz) Note 1	VHF-FM Channel 13 (156.65 MHz) Note 1	VTS Note 1	Command and Control Note 2
WMSL*	X	X	X	X	X	X
WMSM/WMEC*	X	X	X	X	X	X
WAGB/WMSP*		X	X	X	X	X
WIX*		X	X	X	X	X
WLB,WLBB,WTGB*		X	X	X	X	X
WLM/WLIC/ WLI/WLR/WYTL		X	X	X	X	X
FRC/WPB-110*		X	X	X	X	X
WPB-87		X	X	X	X	X
Other CG Vessels under 110' and over 26'		X	X	X	X	X
CG Vessels under 26'	As required by the operational commander					

* When operating in the Alaskan AOR, cutters must also guard 4125kHz.

Note 1: Continuous frequency guard of CH 13 and other frequency as dictated by the VTS

Note 2: Frequency guard as dictated by the operational commander;

Note 3: Non Voice VHF frequency.

UHF-AM: Ultra High Frequency-Amplitude Modulated

Figure 9 - Minimum Radio Frequency Guards onboard Coast Guard Vessels

5. CG Vessel Search and Rescue (SAR) Communications. See Chapter 11 for additional policies on CG SAR communications.

6. CG Cutter Communications.

   a. Operations Normal Reports. Operations normal reports should be conducted per the operational commander. All communications guards should be maintained by a Coast Guard shore authority, unless designated by TACON to the Patrol Commander (PATCOM).

   b. Communication Guard Shift (COMMSHIFT). COMMSHIFTs must be submitted to transfer a communication guard and record message delivery responsibility to another unit. COMMSHIFT record messages not submitted result in missed record messages for the command. The procedures for submitting COMMSHIFT record messages are in Reference (a).

      (1) Shore facilities and mobile units that maintain a communication/record message guard for other units must ensure a contingency plan is in place to address outages and casualties.

      (2) Mobile units deploying for less than 72 hours are not required to submit COMMSHIFT record messages unless shifting to a USN unit.

      (3) Commands must contact the appropriate guarding facility to ensure their COMMSHIFT record message is received prior to the COMMSHIFT taking effect.

   c. Communication Spot (COMSPOT) Report. COMSPOT reports will be submitted when the unit experiences communication difficulties (e.g., lost communications, equipment failure, interference). Reference (a) contains COMSPOT reporting procedures.

   d. Communication Guard List. The communication guard list is used to determine record message guard requirements. Commanding officers will be responsible for maintaining an accurate guard list for Address Indicator Group (AIG), Collective Address Designator (CAD), and task organization assignments.

      (1) Cutters should request and review their command's guard lists prior to deployment and update as necessary.

      (2) Units must ensure the C5ISC is an action addressee on all guard list requests, submittals, and modifications.

   Note: Refer to Pre-Formatted (PROFORMA) Message Handbook, NTP 4 SUPP-2 (series) for further AIG/CAD guidance.

7. Cutter operation of COMSATCOM systems.

   a. For other than testing purposes, COMSATCOM equipment should not be used when terrestrial phone and network services are available

   b. COMSATCOM systems are authorized for mission essential communications only. Mission essential communications include required administrative functions and other communications as authorized by the commanding officer. Commanding officers may authorize personal use on a case-by-case basis per paragraph 11 of Reference (p). Prohibited and inappropriate use of these systems is per definition found in Reference (k).

c. All FBB and Ku-Band Sea Tel systems must only be used for data connections. Cutters must not connect telephones or a STE to any Ku-Band Sea Tel or FBB terminal ports. The CG does not have contract support for terminal voice services on these systems. Therefore, if a voice call is attempted, the CG will be billed. This is an unauthorized procurement per Federal Acquisitions Regulations, and will require the cutter to process ratification documentation for obligating the government without funds approval.

d. Coast Guard Cyber Command must notify Cutters when they approach established airtime threshold and will provide underway connectivity usage reports upon request. To request a "Top Talkers" usage report, cutters may submit a remedy ticket, send Email or call the ITOC.

e. Cutters equipped with KVH Ku-Band terminals have a clear voice over internet protocol (VOIP) telephone service capability and are authorized to use this installed capability. Cutters must observe OPSEC when using the KVH VOIP communication.

f. For all cutters equipped with both Ku-Band and FBB systems, Ku-Band is designated as the primary connectivity system. The Ku-Band system provides superior performance and significantly lower operating cost compared to the FBB system. FBB must be used only when Ku-Band service is not available for one of the following reasons:

(1) The cutter is operating outside the coverage range of the large or small cutter Ku-Band system. Ku-Band coverage maps are available on the C5ISC CG Portal page.

(2) The Ku-Band system is inoperable (e.g. CASREP, mast blockage, weather degradation). Cutters must use Satellite Availability Analyst (SA2) to determine possible courses to mitigate mast blockage before switching to FBB.

(3) The Ku-Band system is secured by the cutter as directed or due to other hazard.

(4) The Ku-Band system terminal is shut down by internal software due to the cutter's proximity to a land earth station using competing spectrum.

(5) When using FBB, cutters must monitor the Ku-Band cause of service interruption and must attempt to restore connectivity via the Ku-Band system immediately upon availability of service.

8. CG Boat Communications. Operations reports are required by shore authority.

a. Underway boats must provide a status report every 30 minutes, unless otherwise established by local command SOPs. A new 30 minute period can be initiated after any communication with the boat is made, it does not have to be 30 minutes from the last operations status report.

b. Operations normal reports must contain current position, operational status, and significant changes in weather, wind, and sea conditions. The operational commander is authorized to modify required reporting information based on operations.

c. Normal operations status reports must be transmitted to the guard unit as "ops normal."

d. Operations status other than normal must be reported to the guard unit immediately.

e. Operational Commanders can extend this requirement to 1 hour if AIS is in place and working, but would be the operational commander's decision to extend it based on their evaluation of operational risk.

9. Exemptions to Operations Normal Reporting Requirements. CG vessels operating under the following conditions are exempted from operations normal report requirements:
   a. When reporting through another unit. That unit must have communications with the shore authority (e.g., When maintaining communication with the on-scene commander in conjunction with a SAR mission. A cutter/boat engaged in a SAR mission and reporting to an on-scene commander must shift its communication guard and reporting requirements to the on-scene commander. The on-scene commander must maintain communication with the shore side Sector Mission Coordinator (SMC); or,
   b. When instructed by proper authority to maintain radio silence. In any case of planned radio silence, the shore facility must be notified. Communication must be re-established when authorized by the issuing authority.
10. Visual Communication.
   a. Visual Watch Requirements. The commanding officer or operational commander must determine the need and assignment of personnel as visual communication watchstanders. Visual communication watchstanders must be trained to use all forms of visual communication, based on cutter requirements (e.g., flags, flashing light). Operational requirements for visual watchstanders, if needed, must be documented in the unit SOP.
   b. Visual Communication Records. When maintaining a visual signal watch, all visual signals used for communications must be entered into the unit communication log.
   c. Signaling.
      (1) When the identity of a ship is established as CG, USN, or as an allied naval vessel, the visual signaling procedures in Communications Instructions Signaling Procedures in the Visual Medium, ACP 130 (series) must be used.
      (2) The procedures for visual communication found in the International Code of Signals (INTERCO), National Geospatial-Intelligence Agency (NGA) Pub. 102, must be used when exchanging calls with ships of unknown registry, merchant ships, and non-allied ships. Note: The prosigns in the ACP 130 (series) noted above have a different meaning than the prosigns in NGA Pub 102.
   d. Flashing Light. Directional flashing light is the transmission of signals by a narrow beam of light such as a signaling searchlight. To reduce the probability of interception, directional flashing light must be the primary method of flashing light communication. Non-directional flashing light is the transmission of signals in all directions by a signal light, such as a yardarm blinker. Non-directional flashing light should be considered the secondary means of flashing light communication, and can be used in situations where the signaling unit desires to signal more than one addressee at a time.
      (1) Between sunset and sunrise 12 inch searchlights should be fitted with a suitable filter and a reducer, except when use of unfiltered light is necessary. When using colored filters, due consideration must be given to the following:
         (a) Use of red filters is preferred as it avoids reducing the receiver's night vision; and
         (b) Use of either red or green filters requires caution; the intent is not to be mistaken for the sidelights of a ship when underway.

(2) Unofficial signaling between operating personnel on CG cutters, boats and stations, using the operating signal "ZWC" as a means of maintaining and increasing operator proficiency is encouraged. ZWC is an operating signal that translates to: "The following is to be taken as applying to personnel on watch only." Unofficial signaling must only be conducted with authorization from the commanding officer or officer-in-charge.

e. Flag Hoist. Unless directed otherwise by competent authority, ships entering or leaving port during daylight hours must display their international call sign on the inboard port halyard. The outboard halyards are left free for hoisting emergency and tactical signals.

T. Aircraft.

1. Aircraft Lost Communication. Aircraft commanders that lose communication with their guard unit must initiate the necessary actions to re-establish communications with the guard unit either directly or through another unit. Area and District Commanders can publish additional policy for alert procedures during lost communication situations. Reference (a) contains sample lost communication procedures.

2. Aeronautical Facility. An aeronautical facility is defined as a land station in the aeronautical mobile service and includes civilian air traffic controls, CG air stations (AIRSTA), Sectors, or other military facilities. If available, CG aircraft must maintain their primary operational communication guard through a CG facility.

3. Air-to-Ground Support. Where practicable, COMMCOM and COMMDET Kodiak must be used for medium and long-range HF air-to-ground support. Local operations (e.g., taxiing, fire/crash truck dispatch) must be conducted on UHF-AM and/or VHF-FM over non-maritime mobile bands.

4. Maritime Mobile Bands. Requests for the installation of maritime mobile VHF-FM equipment or authorization for maritime mobile frequencies at CG AIRSTAs to support air-to-ground communication are not normally approved.

5. CG Aircraft Communication Guards.

a. All CG aircraft must guard the following emergency frequencies while in flight (operations permitting):

(1) International Air Distress (IAD), 121.5 MHz;

(2) Military Air Distress (MAD), 243.0 MHz;

(3) VHF-FM Channel 16 (156.800 MHz).

(4) VHF-FM DSC Channel 70; and

(5) 406 MHz Emergency Position Indicating Radio Beacon (EPIRB)

Note: The use of these frequencies must be restricted to emergency communication or situations where other frequencies do not suffice. Normal communication must be conducted on the appropriate CG or aeronautical unit working frequency.

b. CG aircraft must establish a communication guard with an aeronautical facility or CG shore facility within five minutes after takeoff. Positive communications must be attained prior to communication guard being established.

c. The aeronautical facility accepting the guard for the aircraft must be responsible for maintaining the communication for the aircraft until it lands or until another station has established communication and has accepted communication guard responsibility for the aircraft. It is the responsibility of the aircraft commander to ensure the communication guard unit at the point of departure or arrival is properly notified of the aircraft's movement.

d. When a communication guard is accepted by a CG unit, the communication guard unit must request the following information from the aircraft commander: number of personnel onboard, flight origination, flight destination, and hours of fuel remaining.

e. The CG communication guard unit must provide the aircraft with primary and secondary frequencies or modes of communication and the schedule the conducting flight operations status reports.

f. If a change of communication guard is necessary due to operations or deteriorating communications, the aircraft must ensure the communication guard unit is immediately notified via any means. Failure to do so will trigger lost communications procedures and may result in unnecessary diversion of assets.

g. When the mission is complete or when the communication guard is transferred to another unit, the aircraft commander must notify the previous guard unit. Failure to notify the guard unit of a completed mission or guard transfer can result in a lost communication alert.

6. CG Aircraft Reporting Requirements.

a. Aircraft in flight that have the communication guard with a CG unit must keep the following communication schedules:

(1) Fixed-wing. A flight operations status report every 30 minutes and a position report every 60 minutes:

(a)Normal flight operations status reports must be transmitted as "flight ops normal";

(b) Operations status that is other than normal must be reported accordingly; and

(c)Position reports must include magnetic course, altitude, and speed.

(2) Rotary - Helicopters. A flight operations status report every 15 minutes and a position report every 30 minutes:

(a) Normal flight operations status reports must be transmitted as "flight ops normal";

(b) Operations status that is other than normal must be reported accordingly; and

(c) Position reports must include magnetic course, altitude, and speed.

b. Any communication between an aircraft and the communication guard unit can be used to begin a new reporting period if it includes the necessary OPS or Position required for the next report.

c. When the aircraft maintains communication with air traffic control facilities, the required reports must be made per FAA regulations. Whenever possible, the aircraft commander

must also maintain a guard on CG frequencies if it does not interfere with the primary air traffic control communication.

d. When the aircraft maintains communication with an on-scene commander or officer-in tactical command in conjunction with a coordinated mission, the aircraft commander must make the required position reports to the on-scene commander or officer-in-tactical command. An aircraft engaged in a coordinated mission and reporting to an on-scene commander/officer-in-tactical command must shift its communication guard from the aeronautical unit to the on-scene commander/officer-in-tactical command until released from the coordinated mission.

7. Aircraft and Distress, Urgency, and Safety Communication. Any aircraft required by national or international regulations to communicate for distress, urgency, or safety purposes with stations of the maritime mobile service must be capable of transmitting on 4125 kHz or on VHF-FM Channel 16 (156.800 MHz).

   Note: The safety of life and non-interference exceptions is at the determination of the pilot. In making this determination, the pilot must balance the risk of interfering with a possible distress or safety call by a mariner against the benefits of making the transmission. Non-interference exemptions can include transmissions on channels exclusively allocated to the CG (i.e., VHF-FM Channel 21A (157.050 MHz), VHF-FM Channel 23A (157.150 MHz), VHF-FM Channel 83A (157.175 MHz)) provided that propagation does not overlap any foreign national waters absent permission from that government and that all affected Sectors are aware of the operation. Refer to 47CFR § 87, Aviation Services, the equivalent for aircraft as Part 80 is to maritime.

8. Very High Frequency/Ultra High Frequency (VHF/UHF). VHF and UHF air-to-ground frequencies must be used to the fullest extent possible for short-range communication with the aircraft's parent command. CG VHF and UHF maritime mobile frequencies (Sector RESCUE 21 tactical channels) must be used to the fullest extent practical to communicate with CG boats and Sector shore units. Additional policy regarding CG SAR communication is found in Chapter 11 of this Manual.

   a. Air-to-air use of VHF-FM in the 156-162 MHz maritime mobile bands is not permitted except when no other means of communication exists for the prosecution of SAR or when the need exists for a common frequency between multiple aircraft and surface units. Transmission on NOAA weather frequencies is prohibited regardless of the situation.

   b. In emergencies or SAR situations CG aircraft may use any frequency authorized to a nongovernment facility. Commanding officers should determine what VHF-FM frequencies are used by public safety agencies in their area and submit requests for use per Reference (e). See Chapter 11 for additional policies on CG SAR communications.

   c. Aircraft must use lowest power output required to maintain reliable communication. Higher power can be used in the 156-162 MHz maritime mobile band when necessary.

   d. Aircraft operating above 1000 feet must not transmit on VHF-FM maritime channels (frequency range 156-162 MHz), except for reconnaissance aircraft participating in icebreaking operations which are permitted to operate on these channels up to 1500 feet in altitude.

      (1) Transmissions by aircraft in this band must not exceed five watts.

(2) In the event there is a safety related situation, an aircraft operating above 1000 feet can communicate on these channels provided the communication is as brief as possible and the communication is not likely to cause interference to other communications.

e. Aircraft may broadcast urgent maritime safety information and weather warnings to ships.

(1) District Commanders must determine policy on broadcast content and when such broadcasts are necessary.

(2) No transmission on VHF-FM Channel 16 (156.800 MHz) must be made unless that frequency is monitored from the aircraft and determined to be clear of distress and safety communications.

(3) Transmission duration on VHF-FM Channel 16 (156.800 MHz) must be short and not exceed 60 seconds.

(4) Deviation from the requirements of this Chapter is permissible only when necessary to protect safety of life.

(5) Sector watchstanders and foreign Rescue Coordination Centers (RCCs) must be notified, where appropriate, before commencement of broadcasts.

f. CG aircraft equipped with VHF-FM DSC radios must guard DSC VHF-FM Channel 70 (156.525 MHz).

(1) CG aircraft use of Channel 70 (156.525 MHz) is authorized only for SAR communications with maritime mobile stations in the maritime mobile service. CG aircraft must not use Channel 70 (156.525 MHz) for non-SAR related communications.

(2) Operations permitting, CG aircraft in receipt of an urgent DSC alert must immediately relay the pertinent information to their operational commander via the most expeditious means available.

g. VHF-FM Channel 83A (157.175 MHz) must not be used in the areas where interference with Canadian users of this frequency could occur unless experiencing an in-flight emergency. Refer to 47CFR § 80.57 Canada/U.S.. channeling arrangement for VHF maritime public correspondence and Part 87, Aviation Services.

9. High Frequency (HF). CG HF air-to-ground frequencies must be used for long range communication with COMMCOM. The following HF networks are available for CG aviation use:

a. Secure COTHEN Network (SCN). See paragraph R.2. of this chapter.

b. Sea, Air, Shore Secure (SASS). See paragraph R.2. of this chapter.

c. COTHEN. When available, CG aircraft must use COTHEN as a primary means to maintain reliable communication with COMMCOM.

10. Radio Silence. When the aircraft is instructed by proper authority to maintain radio silence, the following applies:

a. The requirement to maintain a communication schedule with the guard unit is waived. The guard unit must be notified and radio contact reestablished when authorized by the issuing authority.

b. If an aircraft has an in-flight emergency, the pilot in charge must break radio silence to make notification if the aircraft or personnel are at risk.

11. Aircraft Voice Call Signs. Voice call signs for aircraft must be per Reference (i) and appropriate instructions issued by the operational commander. All aircraft on SAR missions and desiring expeditious handling by the FAA must insert the word "RESCUE" in the call sign after CG when using voice procedures.

U. Amateur Radio Stations. Amateur radio is recognized as a means of personal entertainment for recreation and morale. Amateur radio activities are authorized at CG units. Amateur operations must, at all times, remain separate from and independent of any or all CG communications. The procedures for the establishment of amateur radio stations at CG units are found in Reference (a).

V. Military Auxiliary Radio System (MARS). Military Auxiliary Radio System (MARS) is a program supported by the DOD in which U.S. amateur radio stations and FCC licensed operators voluntarily participate and contribute to the mission of providing communications on a local, national or international basis as an adjunct to normal military communications. CG personnel are authorized to participate in the DOD MARS program by establishing MARS stations ashore and afloat. The MARS system handles morale and quasi-official record and voice communications for the armed forces and authorized U.S. government stations throughout the world. The procedures for the establishment of a MARS station at CG units are found in Military Auxiliary Radio System (MARS), DoDI 4650.02.

CHAPTER 6 COMMUNICATIONS SECURITY (COMSEC)

A. General. The protection of government communications not intended for the general public is crucial to effectively plan and execute CG missions. Commands engaged in classified or sensitive operations must exercise caution when communicating with the general public to prevent the release of classified or protected information.

B. Communications Security (COMSEC). Joint DOD Publication 6-0, defines COMSEC as, "Actions designed to deny unauthorized persons information of value by safeguarding access to, or observation of, equipment, material, and documents with regard to the possession and study of telecommunications or to purposely mislead unauthorized persons in their interpretation of the results of such possession and study." Communications security includes cryptographic security, transmission security, emission security, and physical security of COMSEC material. COMSEC provides measures that protect and defend systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

1. Communications Security (COMSEC) Responsibilities. The following are specific roles and documents responsibilities governing overall COMSEC that protect classified and SBU government communication:

   a. Director, Office of Management and Budget (OMB). Director, OMB, as established by Title III of Public Law 107-347, also known as the Federal Information Security Management Act of 2002 (FISMA), is the official responsible for establishing polices for the physical and electronic protection of federal government information whether classified or SBU with two significant exceptions (the Secretary of Defense (SECDEF) and the Director of National Intelligence (DNI)). The OMB, acting through the National Institute of Standards and Technology (NIST), maintains overall policy regarding the safeguarding of SBU including SBU National Security Information (NSI) and the associated security systems.

   b. Secretary of Defense (SECDEF). SECDEF, assisted by the National Security Agency (NSA), is responsible for the protection of classified national security information and the associated systems.

   c. Director of National Intelligence (DNI). DNI is responsible for intelligence related information and systems.

   d. Secretary, Department of Homeland Security (SECDHS). SECDHS is responsible for protection of classified and SBU information on all department systems as directed by OMB or SECDEF.

   e. Commandant (CG-62). Commandant (CG-62) has overall COMSEC responsibility for the CG and serves as the program manager. Commandant (CG-62) coordinates internationally with coalition partners through the NSA and State Department, the other military services, and federal, state, local, and tribal law enforcement agencies to meet encrypted communications interoperability requirements for all CG missions. Commandant (CG-62) must perform the following functions:

      (1) Liaison with Forces Readiness Command (FORCECOM) to promulgate COMSEC procedures throughout the CG;

(2) Promulgate detailed CG COMSEC policy and exercises service-wide management and oversight of Key Management Infrastructure (KMI) accounts;

(3) Function as the CG command authority (CA) for asymmetric key under the NSA Central Facility and function as the Controlling Authority (CONAUTH) for all CG controlled symmetric keys, including those comprising the national level Joint Inter-Agency Counterdrug COMSEC (JIACC) KEYMAT Package.

f. Area Commanders. Area Commanders must manage the CG COMSEC program as follows:

(1) Provide oversight and management of Area COMSEC matters and physical security measures per applicable instructions;

(2) Provide oversight and management of the KMI programs within their AOR per policy provided in this Manual;

(3) Request and approve COMSEC monitoring within their AOR. Area Commanders must maximize use of the information provided by the monitoring agency toward general operations security (OPSEC)/COMSEC training and awareness. Area Commanders, or those individuals acting in these capacities, must personally approve COMSEC monitoring requests within their AOR. This authority must not be re-delegated; and,

(4) Review COMSEC monitoring reports.

(a) Review and evaluate breaches in COMSEC for impact on overall operations;

(b) Report significant COMSEC disclosures observed in these provided reports per section C.6 of this Chapter; and,

(c) Identify and initiate corrective administrative actions as necessary.

g. District Commanders. District Commanders must direct their units per Area COMSEC instructions, and address their COMSEC and COMSEC monitoring needs to the cognizant Area Commander. In addition, District Commanders must:

(1) Provide oversight and management of COMSEC matters per applicable instructions;

(2) Provide oversight and management of the KMI programs within the AOR;

(3) Review COMSEC monitoring reports;

(4) Review and evaluate breaches in COMSEC for impact on overall operations;

(5) Report significant COMSEC disclosures observed in these provided reports per section C.6 of this Chapter; and,

(6) Identify and initiate corrective administrative or punitive actions as necessary.

h. Commanding Officers. Commanding officers must maintain a comprehensive COMSEC program at their commands. Unit commanding officers are responsible for the manner in which their personnel perform KMI/COMSEC duties. Commanding officers must:

(1) Provide oversight and management of COMSEC measures per applicable instructions;

(2) Be thoroughly familiar and comply with the specific responsibilities and duties and required inspections as outlined in Reference (l);

(3) Conduct personnel training emphasizing the importance of preventing unauthorized disclosure of information, both classified and unclassified, in addition to the proper management and security of all COMSEC material held by the command;

(4) Regularly review and evaluate breaches in COMSEC for impact on local and overall operations; and,

(5) Identify and initiate corrective administrative actions as necessary in response to COMSEC incidents and practices dangerous to security.

C. Communications Security (COMSEC) Monitoring. COMSEC monitoring provides the means to detect unauthorized disclosures of classified and SBU government information on non-secure communication circuits and systems. The information provided to the agency being monitored assists in identifying trends, vulnerabilities, and weaknesses. It is not meant for punitive action. Awareness of active COMSEC monitoring of government communication systems is an essential element of deterrence of such disclosures.

1. Communications Security (COMSEC), National Telecommunications and Information Systems Security Directive Number 600 (NTISSD No. 600) is the controlling directive for COMSEC monitoring of government communication systems.
2. All COMSEC monitoring by the CG, or as mutually agreed upon by the CG and another agency, must be conducted in strict compliance with this Manual, NTISSD No. 600, and Reference (k).
3. With limited exception, no agency will monitor CG communication for COMSEC purposes without the express written approval of the Commandant (CG-00EA).
4. Notification of COMSEC monitoring existence can be accomplished by any of the following means, or combination thereof, if the legal officer considers the means chosen to be legally sufficient to achieve proper notification in terms of content, prominence, and specificity:
   a. Decals placed on the transmitting or receiving devices (phone, radios, computers, etc);
   b. A notice in the daily bulletin, plan of the day, or similar medium;
   c. A specific correspondence to users (i.e. an annual ALCOAST from CG-6);
   d. A statement on the cover of official telephone book or communication directory; or,
   e. A statement in the standard operating procedures, communication-electronics operating instructions, or similar documents.
5. Legal Certification.
   a. Commandant (CG-62) must ensure all the legal provisions of NTISSD No. 600 are met, reviewed and recertified every two years with applicable monitoring agencies;
   b. Users of government communication systems must be notified in advance that the use of these systems constitutes consent to monitoring for COMSEC purposes. The guidelines for providing this notification are in section C.4. of this Chapter;
   c. Area legal offices must annually, or when requested by Commandant (CG-62), conduct a legal review of current COMSEC monitoring procedures and must ensure at least one of the list of mandatory methods for COMSEC notifications are in place at each unit within the AOR. When the annual legal review is completed, send report of compliance with NTISSD

No. 600 via record message to Commandant (CG-672) and Commandant (CG-094) no later than 15 July of each calendar year to allow time for extensive legal counsel adjudication; and,

d. Commandant (CG-62) must ensure the CG is recertified so monitoring agencies may, if applicable, legally continue to provide COMSEC monitoring for the CG.

6. Unauthorized Disclosure. Unauthorized disclosure reporting procedures are in Reference (a).

D. Encryption. This section outlines the policy for encryption use for CG communication.

1. Encryption Use. All CG radio communication not intended for the general public must be conducted via encrypted (secure or protected) channels proportionate with the classification level of the information being transmitted or received when the capability is available. The following policy applies:

   a. Classified information must be processed using NSA approved cryptographic equipment and materials; and,

   b. SBU information such as law enforcement sensitive (LE Sensitive), FOUO, protected critical infrastructure information (PCII), sensitive personal identifiable information (SPII), and PII must use NSA and DHS approved equipment and materials or equipment that is NIST/Federal Information Processing Standards (FIPS) certified. Policy for the transmission of SBU information via CGOne is contained in Reference (c).

2. Maritime Public Communication. Maritime public support communications must not be encrypted.

3. Advanced Encryption Standard (AES). CG units must use AES (256 bit) encryption as the primary encryption mode for all SBU tactical communications. CG units participating in multiagency operations or working with other CG units without AES encryption may use DES encryption, as required, for communication interoperability.

   a. AES cryptographic keys must be obtained from Customs and Border Protection (CBP) National Law Enforcement Communications Center (NLECC), Orlando, Florida.

   b. The encryption key may be obtained via over-the-air-rekeying (OTAR) or currently authorized procedures.

4. AES/DES Cryptographic Keying Material (Keymat) Effective Period. The effective date/time for the CG protected voice encryption keys (AES) is the first working Monday of the month at 1900Z. Federal holidays are not considered working days, therefore, if key change day falls on a federal holiday, the key change is automatically postponed until the following Monday.

5. Data Encryption Standard Output Standard Feedback (DES-OFB). The DES-OFB capability must be maintained in all VHF/UHF radios. This provides backward compatibility for unique non-AES encryption requirements.

6. Keying Material and other Government agencies. See Chapter 9, paragraph L., of this Manual for information regarding the use and sharing of encryption keys for interoperability purposes.

7. Encrypted Automatic Identification System (EAIS) Keysets. CG units are authorized to share unclassified EAIS keysets with federal, state, or local port partners and other government

agencies in conjunction with joint port operations. Individual keyset is unclassified (FOUO), and must not be passed through unencrypted means.

a. Areas and Districts must ensure all EAIS-equipped assets under their purview are transmitting the correct AIS information and must update the encrypted keyset on the first day of each month at 1800 Greenwich Mean Time (GMT). Failure to update the EAIS keyset with the correct key at the prescribed date/time, transmitting incorrect AIS information or testing with an unrecognizable (invalid) keyset significantly degrades the CG Common Operational Picture (COP), negatively impacts data sharing and creates the potential for blue-on-blue incidents.

b. Units must test all keyed assets with other locally keyed assets or view the EAIS status website to ensure the equipment is properly keyed and transmitting the correct AIS information. EAIS Status Website: http://avis.osc.uscg.mil/bft/dashboard.html

(1) Operators must allow the equipment to operate for at least 20 minutes in the SECURED TX mode to ensure the encrypted broadcast is captured by the NAIS.

(2) Units transmitting incorrect AIS information and/or an invalid/superseded keyset must be notified via e-mail by the CG NAVCEN, with a copy sent to the appropriate Area C5I division or District communications office.

Note: Refer to Reference (a) for specific EAIS related operating, testing and troubleshooting procedures.

c. Units that provide CG operational EAIS key to authorized port partners must:

(1) Have a written agreement (e.g. MOA/MOU) in place prior to key sharing that addresses, at minimum, distribution, handling, storage, and reporting loss or compromise.

(2) Ensure EAIS keyset distribution to port partners is per policy and that it is distributed only to the correct port partner points of contact.

(3) Check the status of CG EAIS keyed port partners within the unit's operating area via the EAIS status site and take prompt action if keyed incorrectly.

Note: the EAIS status site is not available outside the CGOne network.

E. Over-The-Air-Rekeying (OTAR). All Key Management Facility (KMF) and OTAR services, including any required back-up facilities, for the CG must be with CBP NLECC only. Units are to submit a CGFIXIT ticket for CBP NLECC OTAR and KMF support through CSD. If CSD cannot support the ticket will be escalated to C5ISC.

F. Loss of Tactical Radio or Key Variable Loader (KVL).

1. Units must immediately report the loss of a keyed or unkeyed UHF-VHF tactical radio or KVL to National Law Enforcement Communication Center (NLECC) and the unit's chain of command using the following record message template:

   P XXXXXXXZ mmm yy
   FM: (YOUR UNIT PLA HERE)
   TO: NLECC WSOC ORLANDO FL
   INFO (First unit/command in chain of command)
   (District dt)
   COMLANTAREA or PACAREA
   COGARD C5ISC ALEXANDRIA VA
   COMDT COGARD WASHINGTON DC
   SUBJ: LOSS OF UHF-VHF TACTICAL RADIO OR KEY VARIABLE LOADER (KVL)
   1. (Radio or KVL type), SERIAL NUMBER: XXXXXXXXXX
   2. Radio Set Identifier (RSI) NUMBER: XXXXXXX
   3. (Details of loss)
   4. COMPROMISE CAN or CANNOT BE RULED OUT
   5. (Position of loss and method of determining position)
   6. Any amplifying information deemed appropriate to the loss
   7. Replacement equipment ordered? (Yes/No)

2. If deemed timelier and more expeditious, all the above information may be transmitted by e-mail to the appropriate addresses. The e-mail address for WSOC is: NLECC-WSOC@CBP.DHS.GOV. CG e-mail addresses are in the Global Address List.

3. The unit/command reporting the lost or missing tactical radio should then order a replacement radio from SFLC via MILSTRIP message using Advice Code 5A (no turn in).

4. Additional guidance for lost radios can be located at: https://cg.portal.uscg.mil/units/c3cen/Codeplug-UHF-VHF/SitePages/Home.aspx

G. Communications Security (COMSEC) Material Control System (CMCS). The CMCS includes production facilities, CORs, distribution facilities, depots and COMSEC accounts and was established to effectively account, control, distribute, and safeguard COMSEC material" The CMCS is comprised of two major components:

1. Key Management Infrastructure (KMI). KMI is an interoperable collection of systems, facilities, and components developed by the services and agencies of the U.S. Government to automate the planning, ordering, filling, generation, distribution, accountability, storage, usage, destruction, and management of electronic key and other types of COMSEC material, including cryptographic equipment.

2. Vault, Distribution, Logistics System (VDLS). The VDLS consists of manual and automated systems that operate the vaults and depots that physically receive, store, distribute, and directly handle physical COMSEC material. The Defense Courier Service is a component of the VDLS.

H. Key Management Infrastructure (KMI). The primary source for KMI policy is CMS-1. CG specific KMI policy is promulgated by this Manual and numbered CG communication policy record messages with a COMSEC advisory caveat. The advisory messages are effective until incorporated into the appropriate reference.

1. KMI Roles and Responsibilities. Reference (l) outlines KMI management roles and responsibilities, selection and designation criteria, and the training requirements. To efficiently implement COMSEC responsibility:

   a. All CG personnel performing COMSEC related duties must be thoroughly familiar with applicable KMI documents;

   b. All CG personnel who install, operate, or maintain communication or cryptographic systems must comply with applicable COMSEC and/or NIST publications and directives; and,

   c. CG personnel must immediately report any irregularities that impact COMSEC material as outlined in CMS-1.

2. KMI Program Management.

   a. Commandant (CG-62). Promulgates detailed CG COMSEC/KMI policy and procedures, while exercising service-wide management and oversight of CG KMI accounts. In addition, Commandant (CG-62) must:

      (1) Work closely with NSA, CNO, Naval Communications Security Material System (NCMS), and the KMI Tier 1 entities to ensure all CG KMI accounts have the necessary COMSEC resources to effectively operate;

      (2) Issue KMI procedures and guidance throughout the CG;

      (3) Serve as the COMSEC Service Authority (SERVAUTH) and COMSEC Immediate Superior in Command (ISIC) for all CG KMI accounts. Local account managers must initially contact their designated Area ISIC on KMI matters; and,

      (4) Have primary responsibility for the implementation of the DoN CMS COR audit program.

   b. C51SC Security Engineering Section. Is the action entity for KMI providing select Service Authority services for KMI and oversight for KMI operations, policy, procedures, and training under Commandant (CG-672). Functions include administration and performing COR audits and provision of CG CMS COR Auditors; KMI Operating Account Manager (KOAM) Course of Instruction (COI) coordination; liaison to NCMS, NIW, and other USN entities for KMI and other Department of the Navy (DoN) entities for KMI specific matters pertaining to the CG; standing membership on DoN KMI specific process improvement working groups; Cryptographic hardware management and matters pertaining to cryptographic keying material.

   c. Area Commanders. Area Commanders must assist in the management of the CG KMI Program as follows:

      (1) Designate in writing a KMI ISIC and to assist CG commands in managing their KMI accounts. ISIC responsibilities are outlined in Reference (l);

(2) Coordinate USN/USCG KMI support requirements with the appropriate USN fleet commander and promulgate Area specific COMSEC instructions, requirements, and procedures;

(3) Initiate corrective actions as appropriate in response to COMSEC incidents; and,

(4) Ensure compliance with the Continuous Evaluation Program (CEP) per Reference (q).

d. District Commanders. District Commanders must direct their units per Area COMSEC instructions, to address their COMSEC needs to the cognizant Area Commander. In addition, district commanders must:

(1) Assist CG units within their AOR in managing their KMI accounts as needed;

(2) Promulgate District specific COMSEC instructions, requirements and procedures; and,

(3) Ensure compliance with the CEP per Reference (n).

e. Commanding Officers. Commanding officers are responsible for maintaining a comprehensive KMI program within their command. Unit commanding officers must:

(1) Be thoroughly familiar and comply with the specific responsibilities, duties, and required self-assessments and spot checks as outlined in Reference (n);

(2) Conduct personnel training to emphasize the importance of prevention of unauthorized disclosure of information, both classified and unclassified, in addition to the proper management and security of all COMSEC material held by the command; and,

(3) Ensure compliance with the CEP per Reference (n).

f. KMI Account Manager/Alternate Account Managers. KMI account managers/alternates must:

(1) Be responsible for all actions associated with the KMI account to include receipt, handling, issue, safeguarding, accounting, disposition, and management of COMSEC material;

(2) Serve as the commanding officer‘s primary advisor on KMI account management matters; and,

(3) Comply with specific responsibilities per Reference (l), and all applicable NSA/DON/CG doctrine, policy and procedures manuals.

g. Local Element (LE) Personnel. LE personnel must:

(1) Be responsible to the commanding officer and regional KMI manager for the proper management and security of all COMSEC material assigned; and,

(2) Comply with specific responsibilities per Reference (l) and all applicable NSA/DON/CG doctrine, policy and procedures manuals.

3. Communications Security Material System (CMS) Central Office of Record (COR) Audits. KMI accounts must be audited at least every 24-36 months; beyond 36 months requires a waiver from NSA. KMI account audits must be conducted as per Reference (l) and this Directive. Area KMI ISICs must perform CMS COR audits of KMI accounts under their cognizance and other DON accounts as necessary.

4. Management of Cryptographic Equipment. The repair and replacement of all cryptographic equipment must be coordinated through the C5ISC (ESD-ASB-SE). While specific procedures are detailed in Reference (l), commands are responsible for the proper maintenance and repair of cryptographic equipment, as follows:
   a. Repair of USN owned cryptographic equipment must be accomplished per Annex R of Reference (l); and,
   b. Inoperative equipment must be repaired or replaced by the servicing crypto repair facility (CRF) or other repair/maintenance facility.
5. Regional Communications Security (COMSEC) Key Management Infrastructure (KMI) Account. The regional KMI account is a numbered COMSEC account that interacts with the Common Tier 1, USN, COMSEC Central Office of Record, and other KMI accounts to support itself and multiple Local Elements, both issuing and using.
6. Responsibilities. In regional KMI account operations, all account personnel must have duties and responsibilities for LEs equivalent to their current KMI roles as defined in Reference (l). The following are additional responsibilities:
   a. Maintain a Letter of Agreement (LOA) between the regional account's commanding officer and all LE commands;
   b. Provide all Tier-1/COR functions (e.g., receipts, destructions, inventories) to include provisioning of all key and COMSEC material support to the LE's assigned to their region;
   c. Provide COMSEC oversight, including:
      (1) COMSEC incident reporting;
      (2) COMSEC practice dangerous to security reporting; and,
      (3) Ensure COMSEC allowance meets mission requirements and is delivered in a timely manner.
   d. Develop and sustain a local training program for the LE to maintain personnel proficiency/certification;
   e. Ensure quarterly spot checks are completed on all LEs per Reference (l) and ensure LE(I)s are conducting required spot checks on LE(U);
   f. The regional account must conduct 01 Annex B annually for each LE.
   g. The regional account manager and KMI subject matter expert must maintain professional relationships with program entities, Commandant (CG-62), C5ISC, and Area ISICs and be responsive to inquiries or requests from such as applicable;
   h. The regional account must ensure that all personnel whose duties require them to use COMSEC materials hold and maintain the necessary clearance level and that the privileges assigned formally authorize access to COMSEC material. This requirement must be part of the LOA with the LE(I) who must also require personnel who are issued COMSEC material to complete an SD form 572 Cryptographic Access Certification and Termination per Reference (l);

i. Only the ISIC can provide written certification that the storage facility (i.e. safe and/or vault) is approved for storage of the highest classification of COMSEC material to be stored. The regional account must reference the ISIC approval memo; and

j. Ensure the Personnel Qualification Standard is completed by LE personnel.

7. Local Elements.

a. LE's are hand receipt holders which reside at the Tier 3 layer in the COMSEC hierarchy. A LE(I) receives COMSEC material from an established account and issues material to a LE(U) on a local custody basis. Generally, these LE(I) entities are external to the account but may be internal to the account. An LE(I) performs most normal KMI account functions, without the overhead of a KMI suite. It interacts only with its assigned CG regional KMI account and supported LE(U) for all COMSEC material, electronic key, and COMSEC management functions. LE(U) are directly responsible for COMSEC to either a regional KMI account or to the LE(I) that provides their COMSEC support.

b. Additionally, the LE may have a requirement to build specialized databases to load any of the numerous sophisticated next generation of end crypto equipment units (ECU) fielded throughout the CG.

c. All transactions between a LE(I) and regional account and a LE(I) and LE(U) must use a continuous chain of accountability documents, including issue and destruction reports (i.e., LE(I)s must utilize a COMSEC Material Report (SF-153) or other approved document).

d. A MOA/MOU between the supporting KMI account and LE, the supporting LE(I) and LE(U) must be established when personnel are not part of the same command.

e. Additional requirements are stated in Reference (l).

CHAPTER 7 MESSAGING

A. General. Messaging consists of the various formal record messaging systems. For specific policies on Email, chat or other instant messaging services, and text messaging, please refer to Reference (c). Note: Administrative Official Information Exchange (Admin OIX) has been renamed to Command Email. Command Email was established upon the transition from the Coast Guard Messaging System (CGMS) to the Command and Control Official Information Exchange (C2OIX) system. The former Admin OIX system name was often being confused with the C2OIX system, accounting for the name change from "Admin OIX" to "command Email."

B. MINIMIZE. See Chapter 5, paragraph C of this Manual for details on MINIMIZE policies as they pertain to messaging.

C. Record Messaging. Record messages are one of the methods used by the CG and other government agencies to exchange official information between organizations. Originators must use applicable directives or other instructions to determine if the information to be passed requires a record message or if it may be passed more efficiently via other means (e.g., secure telephone, Email, SIPRnet chat, operational voice circuits); thereby, eliminating the need for the record message.

1. Inviolability of Record Messages. To ensure authenticity, privacy, and security of record message content, distribution of record messages and the location of record message files must be done in a manner that prevents unauthorized viewing or access. At a minimum, each command must employ the following measures to protect record message files:

   a. Place printed record messages on covered boards and in covered files;

   b. Set access restrictions on electronic record message boards; and,

   c. Instruct personnel with record message viewing capability not to discuss record message content with unauthorized personnel.

2. Messaging Roles and Definitions.

   a. Originator. The originator of a record message is the command by whose authority a record message is sent.

   b. Drafter. The drafter is the person who actually composes a record message for release by the releasing officer.

   c. Releasing Officer. The releasing officer is a properly designated individual authorized to release record messages for transmission in the name of the originator. In addition to validating the contents of the record message, the releaser's signature affirms compliance with record message drafting instructions. Commands must specifically designate a limited number of users with record message release privileges during periods of MINIMIZE.

3. Record Message Effective Periods. All record messages, to include general messages, are effective for 90 days only unless otherwise noted within the message text.

4. Internet Release of Record Messages. General Message File (GMF) owners (see paragraph F. below for GMF discussion) are designated as the only authorized organizations to post record messages to the internet. GMF record messages authorized for internet release must have the following statement as the last line of text: “INTERNET RELEASE AUTHORIZED."

a. Record messages without this authorization from the originator must not be posted to the internet or Emailed to non ".mil" Email accounts. For additional direction on internet release of CG directives, refer to the Coast Guard Directives System, COMDTINST M5215.6 (series).

b. Internet released record messages must only be posted on the following website by the designated directory services personnel and select GMF owners: United States Coast Guard (uscg.mil) and;

c. Once internet released information is posted to the official website, individuals may distribute the posted information as they normally would if viewing other public internet sites; and

d. CG GMF record messages or other information found on non-CG internet sites may not be current or accurate and must not be used as a source of official CG information.

D. Command and Control Official Information Exchange (C2OIX). C2OIX is the enterprise record messaging system for CG units for unclassified through Top Secret (TS) message classifications. Command and Control Official Information Exchange (C2OIX) Tactics, Techniques, and Procedures (TTP), CGTTP 6-01.4, provides instruction for the use of the USN's C2OIX messaging system. FORCECOM TTP Division posts electronic copies of this TTP in the CGTTP Library available on the CG Portal.

1. C2OIX must only be used for the exchange of information related to specific actions to execute and directly support strategic and tactical CG missions.
2. CG record messages are official communication and a representation of the command. Therefore, units must determine who requires release authority as a function of their C2OIX accounts.
3. Unit C2OIX system administrators must maintain a list of authorized record message releasers within their command. Contractors working for the CG are not authorized to release C2OIX record messages.
4. Record message drafters must follow the procedures for proper record message format provided in Command and Control Official Information Exchange (C2OIX), Tactics, Techniques, and Procedures (TTP), CGTTP 6-01.4.
5. Record messages in the C2OIX web application or the C2OIX command shared mailbox must not be forwarded to anyone outside of the message Plain Language Address Designator (PLAD) list without direct authorization from the message originator.
6. Users must not forward a C2OIX record message to any Email account outside the uscg.mil domain.
7. C2OIX is a web based application that delivers messages to units via an Email shared folder which allows viewing messages via outlook shared mailboxes. The primary delivery path of C2OIX messages to all units is via CGOne Network.

E. Other Record Messaging Systems. In addition to C2OIX, command Email, and GMF, the following are afloat record messaging systems:

1. Common User Digital Information Exchange System (CUDIXS). CUDIXS provides a bidirectional, digital messaging link between a ship and a USN Computer and Telecommunications Area Master Station (NCTAMS) or Naval Computer Telecommunications Station (NCTS). Cutters equipped with Naval Modular Automated Communication Systems (NAVMACS) use this as their terminal. The link consists of a single Fleet Satellite Communications (FLTSATCOM) half-duplex channel dedicated to synchronous communications between the CUDIXS shore station and the cutter. The system is compatible with C2OIX and processes unclassified and secure traffic up to and including Top Secret (TS). In addition, vessels may send and receive Operator-to-Operator (OTO) messages in free form of up to eighty characters in length. CUDIXS is considered an alternative route (ALTROUTE) for record messaging for underway cutters so equipped.

2. USN Fleet Broadcast. The Worldwide Multichannel Broadcast (WMUL), formerly called Fleet Satellite Broadcast System (FSBS) enables USN, CG, and allied surface vessels to receive C2OIX record message traffic via a one-way (shore-to-ship), jam-resistant satellite communication path. Because it is receive-only, FSBS provides the ability to send message traffic to ships operating in emissions controlled (EMCON) and/or Hazard of Electromagnetic Radiation to Ordnance (HERO) environments. FSBS is installed aboard WMSL, WHEC, WAGB, and WMEC-270 cutters. Reference (r) contains additional operational details for FSBS.

   a. Annex K to each Area OPLAN and Reference (r) requires equipped underway cutters to copy the Navy Fleet Broadcast as a secondary means for message traffic delivery.

   b. Equipped cutters must ensure that the appropriate cryptographic keying material for receipt of the broadcast is available for operations.

   c. Equipped cutters must conduct regular training to maintain efficient operations. COMMCOM's Communications Assist Team (CAT) provides assistance upon request and NAVWAR FSBS Groom Teams can provide training during grooms.

F. C2OIX Record Message Classes. The three classes of government record messages handled by C2OIX are:

1. Class A. Official record messages originated by the DOD, including the CG when operating as part of the USN;

2. Class B. Official record messages originated by U.S. government departments and agencies other than DOD. The CG is included under Class B, except when operating as a part of the USN; and,

3. Class C. Broadcast record messages in special arbitrary form available to ships of all nationalities and containing data consisting of special services, such as navigational warnings, hydrographic notices, weather forecasts, and time signals.

G. Collective Addresses. The term "collective address" refers to a Task Organization (TASK), Collective Address Designator (CAD), or Address Indicator Group (AIG). This service is only available in C2OIX.

1. TASK groups must be established and maintained by the individual units that request the task group implementation.
2. The cognizant authority is the commander responsible for the composition and use of the CAD/AIG. Requests for CAD/AIGs must be submitted via CG FIX IT ticket.
    a. CAD/AIG must have a minimum of 30 addresses.
    b. Cognizant authorities must not request a CAD/AIG unless the AIG will be used at a minimum of 2 times per month. Anything less defeats the purpose because of the requirements for continuous administrative and telecommunications reviewing and updating to insure they remain current.
    c. Cognizant authorities must route any changes to CAD/AIGs through a CG FIX IT ticket.
    d. Cognizant authorities must recapitulate each CAD/AIG at least once per year or when 10 modifications are issued.
    e. The C5ISC is authorized to act in place of the cognizant authority for CG owned CAD/AIGs for the purpose of creation, modification, maintenance, and disestablishment.

H. Staff Symbols. Staff symbols provide routing, processing, and filing guidelines for correspondence and record message systems. Staff symbols are required with Headquarters, Area, logistic centers, service centers, and District PLADs. A list of authorized staff symbols for CG record messages is found in the Standard Distribution List, COMDTNOTE 5605 (series). Staff symbols are no longer required for record messages destined for USN commands.

I. Special Handling Designation (SHD). A SHD is a term inserted following the record message classification level to inform the receiving station the record message requires special handling. Details of SHD use are found in Reference (a).

J. Operational Report (OPREP) messages. All units must comply with OPREP procedures as detailed in Reference (l) and Reference (r) as applicable. Examples of locally generated OPREP messages are found in Reference (a).

K. Speed of Service Objective (SOSO). Per Reference (r), SOSO is an established time frame from release of the record message to the final delivery to the intended reader's record message folder. The roles and responsibilities pertaining to record message SOSOs are described in the following section.

1. Originator Responsibilities. Commanding officers are ultimately responsible for assigning the appropriate precedence before releasing record messages and must ensure the guideline for precedence assignment in Reference (r) are enforced.
2. Addressee Responsibilities.
    a. Addressees with continuous watch capabilities (e.g., command centers) must ensure record message systems are routinely checked for receipt of high precedence record messages.
    b. Units holding record message guards for other units or detachments must maintain appropriate oversight of all unit folders as operations dictate.

c. Addressees without continuous watch capabilities must ensure effective after-hours notification methods are in place to respond to record messages requiring immediate action.

L. Record Message Text. The text of a record message is defined as the section of the record message below the subject line.

1. Use of upper and lower case letters is permitted for the text of CG generated record messages except for Preformatted (PROFORMA) such as CASREP, general administrative (GENADMIN) formatted, and all record messages destined for automatic broadcast (e.g., NAVTEX). Such messages must be drafted in upper case only.

2. Links within the record message text must not exceed 69 characters and must remain on a single line. Links longer than 69 characters can be shortened by using the "short link" function on CG Portal.

3. See Reference (a) for a list of authorized symbols and abbreviations.

M. Tracer Action. A tracer action enables a unit to trace a record message's transmission path to determine the point at which a delay or failure occurred for corrective action to be taken. Procedures for the initiation of tracer actions are in Reference (a). The record message originator must initiate tracer action for record messages reported as non-delivered.

N. High-Precedence Record Message System Testing. Areas must conduct quarterly high-precedence C2OIX record message system testing using the flash precedence to determine record message system performance and unit notification capabilities. Areas must determine the high-precedence test results using the time the test record message populates the addressee's record message folders rather than the time-of-receipt of the test message record message response.

1. Areas must test both classified and unclassified record message systems.

2. Areas must select 12 random units, with emphasis on providing a good cross-section of unit types under varying operational status within AORs.

3. Areas must track the following results of high-precedence tests:

a. Test record message date-time-group (DTG);

b. Addressees;

c. Addressees' operational status;

d. Times of record message folder delivery and time of notification that the record message was acknowledged by the addressees;

e. If applicable, reason SOSO was not met; and,

f. Other problems encountered with the test.

O. Command Email. Command Email is the standardized method for Emailing information between commands. Command Email Tactics, Techniques, and Procedures (TTP), CGTTP 6-01.5 provides command Email procedures. FORCECOM TTP Division posts electronic copies of this TTP in the CGTTP Library available on the CG Portal.

1. Command Email is an Email based system delivered to all units via CGOne Network. Delivery of messages and attachments originated in Command Email requires CGOne network connectivity (including delivery to underway cutters).
2. With the exception of Headquarters, a single command shared mailbox (CMD-SMB-XXXXX [SDL short title]) is established for each command. The creation of additional Command Email mailboxes at units is not authorized.
3. Emails sent using command Email are official correspondence and a representation of the command. For standardization purposes, drafters must enter the unit's CMD-SMB mailbox name in the "From" line of the Email when sending to another CMD-SMB and must use standard message formatting similar to C2OIX for both the subject line and the message text. However, unlike C2OIX, there are no character or individual line character length restrictions within the text of a command Email message.
4. Command Email does not support the use of operational collective addresses (see paragraph D.8 above) that are used in C2OIX. Originators with a requirement to send Emails routinely to multiple units are encouraged to locally develop personal distribution list. Requests for centrally created mass distribution lists that contain multiple command Email addresses through CGFIXIT will be denied.
5. Sensitive, but unclassified (SBU) and personally identifiable information (PII) may be transmitted via command Email. Therefore, commands must restrict personnel access to the unit's command Email mailbox to command cadre and designated administrative staff on a "need to know" basis.
6. Emails in the command Email shared mailbox must be treated as official CG information and must not be forwarded to anyone not on the original distribution without direct authorization from the message originator. In addition, users must not forward any command Email messages to any Email account outside the uscg.mil domain.
7. Each unit must designate a minimum of two organizational admins/distribution group owners to manage the unit Command Email shared mailbox.
8. For additional guidance on the use of Email for official correspondence, see Chapter 7 of the Coast Guard Correspondence Manual, COMDTINST M5216.4 (series).

P. General Message File (GMF). The General Messages File contains record messages intended to meet recurring requirements for the dissemination of information to predetermined, large standard distribution lists of recipients. The CG Portal General Message File (GMF) page is used for GMF posting. GMF is not delivered via C2OIX or command Email.

The GMF is located under References on the CG Portal home page.

1. General messages have specific titles used to determine their distribution and are assigned a consecutive three-digit serial number followed by a single slant and the last two digits of the current calendar year. General message titles are:
   a. All Coast Guard (ALCOAST);
   b. ALCOAST Commandant Notices (ACN);
   c. All CG officers (ALCGOFF);

d. All CG enlisted (ALCGENL);

e. All CG Personnel Service Center (ALCGPSC);

f. All CG reserve (ALCGRSV);

g. All CG finance (ALCGFINANCE);

h. All CG recruiting (ALCGRECRUITING);

i. All CG Safety (ALSAFETY):

j. Operating Facility Change Order (OFCO); and

k. USN or Joint originated general messages.

2. General Message File Originators.

   a. Coast Guard (CG) Originators. Commandant, Vice Commandant, headquarters Flag/Senior Executive Service positions, Area and District Commanders, Force Readiness Commander, Director of Operational Logistics, National Command Center, the Master Chief Petty Officer of the CG, and Commander, CG Personnel Service Center, concerning matters under their authority. These principals may delegate this authority by name to persons to act on their behalf. Such delegation must be provided via memo to the Vice Commandant, Commandant (CG-09) and the Office of Information Management, Commandant (CG-61).

   b. USN Originators. CNO, Secretary of the Navy (SECNAV), Commander, Navy Information Forces (NAVIFOR), Commander, Naval Security Group Command (COMNAVSECGRU), fleet, forces, and type commanders; and,

   c. Joint. CJCS, joint staff, and joint or unified commanders.

3. GMF Record Message Cancellation. GMF record messages are effective for 90 days unless otherwise indicated per the guidance below. GMF record message cancellation is the responsibility of the originator.

   a. For some general record message series, the first record message released in the calendar year is a recapitulation message. The recapitulation message designates which record messages for that series remain in effect. By omission, all general messages of the series not listed as effective at the beginning of a calendar year are canceled.

   b. Interim cancellation of a general message may be sent at any time during the year. An individual general message, numbered or unnumbered, may include its own cancellation date within the text. In addition, a subsequent message of the same general message series may cancel the general message.

   c. General messages of a series that do not have a yearly cancellation message (historically) and that have not been assigned a specific cancellation date are automatically canceled at the end of 90 days. This period may be extended by a subsequent general message of the same series issued within 90 days of the original message assigning a date when the message is to be canceled. If 90 days have passed and no extension of time has been issued, a general message of this type must be reissued to remain effective.

4. CG GMF Record Message Review/Recapitulation.

a. For all CG General Messages, originators must review their posted information for applicability throughout the year and immediately revise or cancel any outdated information.

b. Originators must transmit an annual recap of their effective general record messages no later than 31 January of each calendar year.

5. GMF Applicability and Distribution. Headquarters units and Area staffs must ensure routing guard lists for general messages remain accurate.

Q. Electronic Mail (Email). Per The Coast Guard Correspondence Manual, COMDTINST M5216.4 (series), Email may be used to transmit official correspondence and constitutes an agency record.

1. Guidance for Email produced or received by CG personnel in the performance of their duties is in Reference (c).

2. Guidance on the personal use of Email is found in Reference (k).

R. Chat or other Instant Messaging Services. Chat services are on-line collaboration tools, used on classified and unclassified systems, where two or more units pass operationally significant information in near real time to supplement voice communications, record message traffic, and tactical data systems. The following policy applies:

1. Skype for Business on CGOne is protected up to the level of UNCLAS FOUO/SBU information;

2. Area, District Commanders and commanding officers must specify requirements for operational employment of chat in their Annex K to Area OPLAN, Operational Tasking (OPTASK) Communications, or unit SOPs; and,

3. When directed by Annex K to Area OPLAN, OPTASK, or SOP, chat sessions must be recorded and saved as a communications log per Chapter 8 of this Manual. In addition;

a. Commanding officers are directed to copy chat discussions including time stamps into official logs as a record of decisions and orders promulgated via chat; and,

b. Commanding officers must ensure that current CG policies concerning sanitation and classification of information within case logs is adhered to, including proper use of classification markings.

S. Text Messaging. Text messaging services are available on a wide variety of mobile communication devices allowing users to pass information in near real time to one or more recipients. Text messaging is frequently used to supplement voice communications, record message traffic, and tactical data systems. Text messaging can be used for operational purposes under the following circumstances:

1. Area, District Commanders, and commanding officers must specify requirements, to include OPSEC implications, for operational employment of text messaging in their Annex K to Area OPLAN, OPTASK Communications, or unit SOPs; and,

2. When directed by Annex K to Area OPLAN, OPTASK, or SOP, significant text communications must be recorded (manually if necessary) and saved as a communications log per Chapter 8 of this Manual.

CHAPTER 8 UNIT COMMUNICATIONS ADMINISTRATION RECORD KEEPING, INSPECTIONS, AND REPORTS

A. General. This Chapter provides policy on communications record administration to include recording and monitoring of communications, records/reports, log keeping, retention and disposal, inspections, and false alert reporting.

B. Recording or Monitoring Equipment.

1. Department of Homeland Security Policy. Telephone calls may be monitored or recorded for legitimate business purposes such as providing training, instruction, or protection against abusive calls. Personal phone conversations and business telephone calls will not be routinely monitored. Exceptions are detailed in paragraph B.3., below. See also Communications Security, Chapter 6, paragraphs B. and C., for amplifying information.

2. Recorded Announcements/Voicemail. Approval is not required to use equipment installed on telephone lines that provide a recorded announcement or voice mail service.

3. Recording of Voice Communication Circuits. Digital voice logger (DVL) and RESCUE 21 recording equipment is required at all tactical operational units (less stations, aircraft, and vessels under 87 feet in length) to record all telephone and voice radio communications where such communications relates to the safety of life and property, including, but not limited to air safety, maritime safety, SAR, and CG tactical communication operations. If the recording contains protected or secure communications, the recording must be safeguarded per References (e) or (p). The CG does not require beep tones or prior consent for the recording of these conversations.

4. Authorization to install and use monitoring equipment for situations not listed in this section must be obtained from the unit servicing legal office.

C. Communication Reports. Procedures detailing communication reports are found in References (a) and (d). These procedures include submitting the following reports:

1. Joint Spectrum Interference Report (JSIR) - Report of Radio Interference; and,

2. Report of Violation of Radio Regulations or Communications Instructions, Form CG-2861A.

D. Communication Records.

1. Intra/Inter-Area Dedicated Circuits. The C5ISC and Base C4IT department Designated Agency Representatives (DAR) must maintain records of all intra/inter-area dedicated circuits. These records must include, at a minimum, the following:

   a. Circuit number;

   b. Carrier identification (indicate if CG owned);

   c. Termination points: Identify facility and geographical location of each user of the circuit (e.g., CG Sector Los Angeles/Long Beach, San Pedro, CA);

   d. Termination equipment: List all terminal equipment used on the circuit, indicating leased or CG owned;

   e. Program supported;

f. Identity of the circuit's use or function (e.g., remote radio-control, teletype, FAX, voice);

g. Monthly recurring cost of the circuit; and,

h. Circuit Telecommunications Service Priority (TSP) level.

2. Communication Logs. Communication Log, Form CG-2614A, is available in the CG Forms Library on the CGPortal. Use of this form is not mandatory. Units using other means for daily communication logs must meet the minimum communication log content requirements established in section D.2.e of this Chapter.

   a. Daily Communication Logs. Daily communication logs must be maintained for all operational units, including CG Auxiliary and deployable mobile communication assets. The following are excluded from this:

      (1) Vessels 65 feet and over not equipped with a recorder or dedicated communication watch. The bridge smooth log may be used for abbreviated communication entries;

      (2) Vessels under 65 feet in length;

      (3) Aircraft, except when acting as on-scene commander;

      (4) Unit vehicles with installed communications equipment; and,

      (5) Personnel deployed with handheld communications equipment.

   b. Complete Log.

      (1) Radio equipped units without recording equipment are required to maintain a manual complete log (paper or electronic);

      (2) Units with recording capabilities (e.g., , RESCUE 21 system, DVL) must maintain a manual complete log (paper or electronic) only when the recording capability is inoperable;

      (3) Corrections to a paper or electronic complete log are not authorized after operator signature; and,

      (4) All radio equipped units must hold quarterly training on maintaining a complete manual log in the event of a recorder casualty.

   c. Abbreviated Log.

      (1) Units with recording capabilities (e.g., RESCUE 21 system, DVL) must maintain an abbreviated log; and,

      (2) Corrections to abbreviated logs are authorized after signature to maintain consistency with recorded logs.

   d. Radio Logs (RADLOGS). Units equipped with RADLOGS must follow the log keeping policy of this Chapter when applicable. RADLOGS meets the abbreviated log requirement for units with recording devices.

e. Daily Communication Log Content.

(1) The following information, at a minimum, must be included in communication logs:

(a) Unit name (use record message plain language address designator (PLAD);

(b) Call sign;

(c) Date and time (Coordinated Universal Time (UTC), expressed as ZULU). The watchstander must obtain an official time check at the beginning of watch to ensure the clocks are accurate. This can be obtained from NIST at www.time.gov;

(d) Frequency/channel;

(e) Communication information (e.g., voice communication, distress alarms, record messages sent/received, broadcasts, equipment outages affecting communication);

(f) Communications equipment and circuit status; and,

(g) Equipment Check results.

(2) Electronic or handwritten log entries must not be erased.

(3) If handwritten, all entries must be in blue or black ink.

(4) Changes to handwritten or electronics logs must be made by drawing a single line in ink or using the strike-through function (electronic versions) through the original statement. The new entry must be made adjacent to the original entry. All changes to the handwritten communication log must be initialed in ink. An electronic log that contains strike-through changes must be printed and initialed in ink next to the change entry.

(5) Signatures are only required if the computer software on a computer generated log cannot permanently lock the data in a file as "read only" at the conclusion of the watch or log. Authenticity of computer generated logs must be maintained.

(6) Use of standard acronyms, abbreviations, designators, symbols, and signals appearing in official publications (e.g., Allied Communication Publications (ACP), NTPs, and ITU publications) is authorized.

(7) Units must log all distress, urgency, or safety signals and related communications regardless of the type of log maintained. Ensure abbreviated log entries for distress, medical communications (MEDICO), and urgent signals include the originator, frequency, time, and a brief synopsis of what occurred. The log can make reference to the recorded log for more information, as required. Events must be logged until it is apparent the unit will not participate in the assistance (e.g., outside AOR).

(8) Units must include cell phone communications in the daily communication log when the cell phone conversation pertains to distress, urgency, safety signals, and related communication.

(9) Significant chat sessions or text communications must be recorded (manually if necessary) and saved as a communications log.

(10) Supervisors must review all communication logs (less recorded logs) for completeness and accuracy prior to submission to the commanding officer.

(11) Units must perform and log a test of electronic voice logging systems once every 24 hours.

Note: Communication log entry examples are found in Reference (a).

E. Retention of Files, Reports, Records, and Logs. Reference (p) prescribes policies and procedures for administering the CG Records, Forms and Reports Program for the lifecycle management of both paper and electronic documents.

1. Incidents of National Significance. Incidents of national significance have permanent retention requirements. Communication records qualifying for permanent retention must be transferred to the National Archives upon completion of documentation project as outlined in the USCG records disposition schedule. These records include incidents or cases identified as having historical significance due to the scope or nature of the case, or cases involving prominent persons. Examples include:

   a. Cases involving prominent persons of national or regional context;

   b. Cases receiving national or regional media attention;

   c. Cases used in Congressional or other oversight investigations;

   d. Cases involving a great number of persons seeking rescue;

   e. Incidents of national significance such as a terrorist attack or natural disaster; and,

   f. Cases representing substantive change in agency policy and procedures.

2. Communication Records Directly Relating to Outstanding Exception, Claim, Litigation, or Investigation. Communication records directly relating to an outstanding exception by the Government Accounting Office, an outstanding claim for or against the U.S., a case under litigation, or an incomplete investigation, must not be destroyed until final clearance or settlement is determined.

   a. Occasionally, a claim or lawsuit is filed against the CG as a result of the assistance provided. The statute of limitations allows citizens the right to submit a claim or lawsuit for a period of time (normally 18 months after incident). The commanding officer/officer-in-charge of the case must consult with the CG legal office to determine if the incident audio file is required to be retained more than 30 days.

   b. If retention is required, ensure all files pertaining to the case or incident are retained until the claim or pending matter is resolved.

3. Historically Significant Case.

   a. Those having historical significance due to the scope or nature of the case, or cases involving prominent persons are retained permanently and must be forwarded to the Director of Governmental & Public Affairs, Commandant (CG-092).

   b. All other case communication records not having historical significance must be transferred to the FRC three years after final closing of the case. These records can be destroyed 10 years after final closing of the case.

4. Audio Files. Audio files consisting of recorded radio transmissions and telephone calls must be retained for 30 days, unless the audio file meets the retention requirements in sections E.1, E.2, or E.3 of this Chapter.
5. Joint Spectrum Interference Report (JSIR) – Report of Radio Interference. JSIRs must be retained for 3 years. See Reference (d) for additional information.
6. Report of Violation of Radio Regulations or Communication Instructions, Form CG-2861A. All violation reports must be retained for 3 years from the date of the incident. See Reference (d) for additional information.
7. Record Messages.
   a. CG Originated Record Messages. The originating office and action office must retain the record message (paper or electronic) for a minimum of 90 days or until the information contained in the record message is no longer effective, whichever is longer.
   b. General Record Messages. CG originated general record messages must be maintained by the originator for 1 year after the date of promulgation.
   c. Address Indicating Group (AIG)/Collective Address Designator (CAD) Promulgation, Modification, or Recapitulation Record Messages. CG generated AIG or CAD promulgation, modification, or recapitulation record message, and all those originated by DOD/DON used by CG units, must be maintained by the C5ISC until cancelled by the promulgating authority.
   d. Record Message Tracer File. Retain for 6 months following resolution.
   e. High-Precedence Message Test Results. Retain for 1 year.
8. Communication Logs. Cutters retain for 90 days; shore units retain for 6 months.
9. Administrative and Non-Essential Communication Records. Retain for 90 days.
10. Communications General Files. This includes plans, reports, and other records pertaining to equipment requests and communication service. Retain for 3 years.
11. Communications Operational Files. This includes record message registers, performance reports, and daily load reports. Retain for 6 months.
12. Telephone Use (Call Detail) Records. This includes such information as the originating number, destination number, destination city and state, date and time of use, duration of the use, and the estimated or actual cost of the use. Retain for 3 years.

F. Disposal of Files, Reports, Records, and Logs. All communication files, reports, records, and logs can be destroyed without report (e.g.,. burning, shredding), if the following criterion is met:
   1. Documents do not require transfer to the FRC; and,
   2. Documents meet the specified retention requirements per this Manual and Reference (s).

G. Communication Readiness. Commands and supervisors must maintain a cognizant relationship with their communication representatives at the Sector, District, and Area level. Area and Districts are required to conduct unit outreach to their port partners and subordinate units to meet stakeholders, establish working relationships, discuss C5I challenges/issues, and harvest new requirements that

will be incorporated in a C5I priorities memo that is submitted to CG-6 and CG-7 annually. Sector Communications Supervisors should mirror the same outreach and engagement to port partners and subordinate units to foster relationships, identify needs, and provide assistance to junior communicators.

H. False Alert Violation Reporting Policy. The following section covers policy for false alert violation reporting.

1. General. As stated in 14 U.S.C. § 521(c), it is a federal felony, punishable by significant imprisonment and/or a monetary fine for anyone to knowingly and willfully communicate a false distress message to the CG or cause the CG to attempt to save lives and property when no help is needed. Unless a false alert is handled as a hoax case as defined in Reference (c), a radio violation report should be submitted per Reference (d) for any violations in the U.S. SAR areas of responsibility, to include:
   a. Deliberate transmission of false alerts;
   b. Inadvertent transmission of a false distress alert without proper cancellation;
   c. Failure to respond to a distress alert due to misuse or negligence;
   d. Repeated transmission of false alerts; or,
   e. Transmission of a distress alert using false identity.
2. Foreign Ship Violations. Contact the FCC regional or national offices to determine if they handle radio violations from foreign ships. If so, submit violation reports to the FCC. If not, violation reports should be submitted per Reference (d).
3. False Alert Feedback Solicitations. The procedures for false alert feedback solicitations are found in Reference (a).

CHAPTER 9 COMMUNICATION PLANS AND EXERCISES

A. General. Communication planning is necessary to help ensure the CGCS is capable of meeting CG mission requirements. The goal of communication plans is to support mission execution by prescribing the effective use of available communication tools. Mission success can best be supported through the development and exercise of thorough communication plans, to include interoperability plans detailing procedures for multi-agency coordination and contingency plans for continued operations in the face of substantially degraded information systems and networks.

B. Communication Planning Information. When developing communication plans, the following items should be considered:

1. Communication capabilities of CG and/or other assets assigned;
2. Communications Security (COMSEC) requirements;
3. Interoperability considerations with state and local law enforcement and emergency response agencies;
4. Radio Frequency plans;
5. Contingency Communications plans;
6. Merchant ship and recreational vessel communication capabilities vary significantly depending on vessel type, scope of operations, and intended use;
7. Communications planning and organization in response to incidents of national significance are addressed within the National Incident Management System (NIMS); and,
8. Regular exercise of the plan ensures operational suitability and accuracy.

C. Radio Frequency Plans. The C5ISC established CG-wide VHF and UHF standard radio frequency plans. All units with mobile and portable VHF and UHF tactical radios must develop and maintain radio frequency plans, to include details for use of all fixed and mobile radio frequencies used by the unit for routine and non-routine operations.

D. Area/District/Unit Communication Plans. Areas, Districts, and units must prepare and issue communication directives appropriately for the organizational levels as specified below. Plans should be reviewed and reissued biennially.

1. Area Communication Plans. The Area Commander must prepare and promulgate area communication plans as Annex K to Area OPLAN. Annex K to Area OPLAN provides tailored communications policy, operating procedures, and general information. Annex K to Area OPLAN will satisfy the requirements of Reference (q) and must include the following:
   a. Unit(s) record message guard, drafting, and releasing responsibilities;
   b. High-precedence record messaging test procedures;
   c. Cutter, aircraft, shore-side, and Auxiliary communication (include operations normal reporting requirements);
   d. Lost communication procedures for cutter, aircraft, and shore-side;
   e. Broadcast notice to mariners (BNM) schedules and special broadcast instructions;

f. List of units and call signs;

g. COMSEC roles and responsibilities;

h. Policy and procedures for use of MILSATCOM circuits;

i. Operational use of cellular and satellite phones;

j. Casualty reporting and restoration procedures;

k. Landline circuit/network arrangements and/or configurations to include use of chat rooms, instant messaging and intercom circuits (e.g., RESCUE 21 and COTHEN);

l. Radio frequency planning and frequency authorization procedures and references;

m. Emergency preparedness activities;

n. Contingency communications, COOP procedures and activities;

o. Interoperability with the USN, DHS, federal, state, local, and tribal governments (e.g., land/mobile radio, first responder);

p. Communications officer or communications supervisor duties;

q. Unit communications inspection checklists;

r. Procedures for obtaining foreign language interpreters to include Auxiliary program;

s. Interference resolution procedures and point of contact resource list (e.g., Joint Spectrum Interference Reports (JSIR); and,

t. Procedures for requesting additional communication resources and obtaining operational approval following the C5I Requirements Management Process.

2. District Communication Plans. District communication plans must be issued either as a supplement to Annex K to Area OPLANs or as a District Annex K. Requirements for content are specific to each District, but generally follow the format of Annex K to Area OPLAN and must satisfy requirements found in Reference (q).

3. Unit Communication Plans/Standard Operating Procedures (SOP). Individual commands must prepare locally-generated communication plans or SOPs, aligned with the Area Annex K to Area OPLAN and District supplements or District Annex K. These plans or SOPs will identify administrative requirements, frequency plans, Continuity of Operations (COOP), interoperability, COMSEC, and operational procedures unique to the unit. Duplicate material found in other publications only as necessary in the interest of completeness.

4. Communication Annex to Operational Order (OPORDER). An OPORDER is designed to support a particular, usually short-term, operation. The communication annex can vary in content and complexity depending upon the scope of the operation, composition of forces and communication capabilities of the participating units. Instructions for the preparation and promulgation of an OPORDER are found in Reference (q).

E. Incident Management Communications. The U.S. Coast Guard Incident Management Handbook (IMH), COMDTPUB P3120.17 (series) provides communication responsibilities and policy for CG personnel during response operations. The designated Communications Unit Leader (COML) should be responsible for developing plans and obtaining, distributing, and supporting operation of computer and radio incident communications equipment and the data management infrastructure.

F. Interoperability Planning. It is critical for CG assets to facilitate interoperable communications with federal, state, local, and tribal partners. DHS defines interoperable communication as "the ability of different components to communicate with each other as necessary, utilizing information technology systems and radio communication systems to exchange voice, data, and video in real time, as necessary, for acts of terrorism, daily operations, planned events, and emergencies."

1. It is the CG's responsibility to ensure its assets have interoperable communications with other federal agencies, public safety providers, law enforcement, firefighters, and emergency management response teams with which we conduct interagency operations.
2. Commandant (CG-672), serves as coordinator for CG public safety interoperability communications.
3. Formal Agreements. A written formal agreement in the form MOU or MOA must be established with each partner agency. Memoranda of Understanding/Agreement, COMDTINST 5216.18 (series) contains CG guidelines for establishing MOUs and MOAs. See paragraphs I. and J. of this Chapter for additional information.
    a. The written agreement should include shared channels/frequencies, facilities, and/or assets, address COMSEC, delineate any/all limitations on circuit use, provide a valid time period, and list both CG and partner agency POCs;
    b. All written agreements will be held on file at the District communications office and copies forwarded to C5ISC, the appropriate Area C5I division, and the applicable Sector;
    c. Agreements will be reviewed with partner agencies on an annual basis (the anniversary of the original date) and rewritten if necessary.

G. Interoperability (IOP) Communication Plans. All units requiring communications with agencies outside the CG must maintain an accurate IOP Communication Plan for rapid and reliable communications during interagency operations with federal, state, local, and tribal partners. The IOP Communication Plan must be kept up-to-date to ensure availability for immediate use by first responders and contingency communication teams. Use the following key points when developing the plan:

1. Include map(s) with partner agency locations;
2. List all partner agencies; develop interagency relationships; identify and contact all external agencies that conduct operations with the District and/or Sector Command Center and maritime/air assets;
3. Develop a communications matrix. List partner agency's capabilities and the full capabilities of all CG assets in the District/Sector and how they interact with partner agencies;
    a. Include the required means of communication for voice and data systems. Detail how to use, deploy or program existing radio/data systems and gateways;

b. Identify the type and extent of information that should be shared;

c. Determine what frequencies to use. Consider using partner agency's system and frequencies or use CG assets and frequencies. OEC publishes the National Interoperability Field Operations Guide (NIFOG) as a reference guide for public safety radio technicians and communication planners. The most recent version of this guide is available via the Commandant (CG-672) Portal Site on the Communications Interoperability page; and

4. Use information from other Districts/Sectors to consider improvements to the IOP Communication Plan.

5. Exercise the plan at least annually.

H. Rescue 21 (RESCUE 21) Mixed-Mode Patch Circuits. Use of the CG's short range communication infrastructure, RESCUE 21, for interoperability is allowed on a not to interfere basis with SAR and Maritime Safety Information (MSI) Missions. However, when using mix-mode patch circuits, the following caveats apply:

1. SBU and FOUO information can be discussed over a landline telephone and by extension over a protected radio circuit patched to a landline telephone; and,

2. If the CG or a partner agency adds a cellular telephone or an unprotected radio circuit to the patch, then the entire patch will be considered unprotected and must not be used to discuss SBU and FOUO information.

I. Contingency Communication Plans (CCP). Operational commanders must develop and maintain a CCP for communications equipped units within their AOR to ensure expeditious restoration of communications in a contingency situation, to support local operations, and to protect the safety of life and property.

1. The CCP should include contingencies for operating in areas where it is known that there are limited or no communications coverage;

2. Each CG District and Sector is unique and must have a tailored CCP for the unit's AOR to include a plan for establishing and maintaining interoperable communications with local partners;

3. COMMCOM is available and should be listed as a source for unit CCP needs.

J. Participation in Federal, State, Local, or Tribal Wireless Voice Networks. Connecting a CG radio communication asset (HF, VHF, and UHF) to a federal, state, or local agency's interoperability system (e.g., Integrated Wireless Network (IWN), Enterprise Land Mobile Radio (ELMR), 800 MHz, HF/VHF, trunked or conventional) is authorized.

1. This connection may be made permanently or on an as-needed basis.

2. Circuits must be considered unprotected unless there is assurance of end-to-end encryption.

3. Whenever possible, units must use a common frequency already authorized for both the CG and federal, state, local, and tribal partners. Maritime band use must be per Reference (d).

4. Any use of CG frequencies by non-government agencies must be authorized in writing by the C5ISC and they must only be used for communication with CG assets. Units must coordinate this use through their District frequency manager.

5. CG use of public safety frequency license, particularly the public safety bands (700/800 MHz), must be certified as necessary in writing by local partners per Reference (e).
6. CG use of a radio provided by federal, state, local, or tribal agency or other compatible radio (handheld or mobile) is authorized.

K. Radio Frequency Administration. Units must notify their District spectrum manager for further coordination with District communications office prior to adding new frequencies to code plugs, authorizing additional users to current CG frequency authorizations, or using another agency's radio frequency.

1. National Mutual Aid Channels. Within the 700/800 MHz public safety spectrum, there are National Mutual Aid channels designated by the FCC for nationwide public safety interoperability with the same frequency and channel naming conventions regardless of the geographic location. These channels in the 700 MHz band (762-775/793-805) and the 800 MHz band (806-809/851-854) include provisions for CG use for regional and local interoperability. This use requires establishment of a formal agreement with the Federal Communications Commission (FCC) Regional Planning Committee (RPC), and state or local government agency. There are 55 RPCs established by the FCC responsible for coordinating interoperability for their respective region. Information on the RPCs can be found at: https://www.fcc.gov/general/700-mhz-rpc-directory-0 and https://www.fcc.gov/general/800-mhz-rpc-directory
2. Per 47 C.F.R. § 2.103(a), Federal agencies are authorized to use non-Federal frequencies (i.e., 700/800 MHz) if the Federal Communications Commission finds that:
   a. Federal operation on non–Federal frequencies shall conform with the conditions agreed upon by the Commission and NTIA;
   b. Such operations shall be in accordance with Commission rules governing the service to which the frequencies involved are allocated;
   c. Such operations shall not cause harmful interference to non–Federal stations and, should harmful interference result, that the interfering Federal operation shall immediately terminate; and
   d. Federal operation has been certified as necessary by the non–Federal licensees involved and this certification has been furnished, in writing, to the Federal agency with which communication is required.
3. Any use of a non-federal frequency by CG units for interoperability communications with a nonfederal agency requires a written agreement between the District and the non-federal agency possessing the license.
   a. The agreement must be in effect for five years and must be renewed for continued operations.
   b. This information can be a part of the standard MOU/MOA referenced above in paragraph F.3 of this Chapter.

L. Encrypted Communications with Partner Agencies.

1. Keying Material (Keymat) Use. Although AES 256 is the primary encryption mode for CG operations, DES-OFB may be used if participating in multi-agency operations.

2. Keying Material (Keymat) Sharing. The following applies to the sharing of CG Type III AES keymat with partner, federal, state, or local government agencies;

   a. Units conducting tactical communication operations with partner government agencies must use the designated AES interoperability (IOP) keymat obtained from CBP NLECC. If AES IOP keymat is not available, or the capability to use AES IOP keymat does not exist, and performing protected communications operations is required, units are authorized to share CG tactical Type III AES keymat with other government agencies.

   b. CG tactical keymat must not be shared with another government agency if other means to protect the communications exist. It must only be used in the most urgent situations and only if the capability to use AES IOP keymat does not exist.

   c. Units must consider all options available for the use of AES IOP keymat, such as CG portable, mobile, and low site radios. These radios can hold more than one encryption algorithm and multiple encryption keys.

   d. If at any time, AES IOP keymat capability becomes available for both the CG asset and the partner agency, CG AES must no longer be used for interoperable communications. The CG AES keymat must immediately be removed from the partner agency radios. The designated AES IOP (FEDIOP or IOP) keymat must then be used.

   e. Units must establish a written agreement per paragraph F.3., of this Chapter, with the partner government agency (i.e. MOA, MOU, LOA) outlining when and for what purpose use of CG AES keymat is permitted. The agreement must state the requirement to safeguard the key appropriately and prohibit dissemination. Finally, it must include an immediate notification requirement to the cognizant command center upon loss of a radio holding CG tactical keymat.

M. Other Government Agency Keying Material (Keymat) in Coast Guard Radios. The loading of other government agency keymat is authorized in CG radios for special operations. This must be coordinated with the District Communications office.

N. Project 25 (P25). P25 is a suite of standards for land mobile radio (LMR) digital radio communications for use by federal, state/province, and local public safety agencies in North America to enable them to communicate with other agencies and mutual aid response teams in emergencies.

   a. Although many government agencies are adopting the P25 standard, no digital communication standard exists across all state and local agencies;

   b. All LMR systems must comply with P25 (P25, EIA/TIA-102) standards where applicable;

   c. All CG radios procured must comply with P25 narrowband requirements and permit use of digital encryption including DES-OFB and AES 256.

O. Communication Exercises. All units must conduct annual exercises to test the implementation of their CCP and/or IOP.

   1. Communications exercises may be completed by either the communications team or as part of a larger exercise.

2. At a minimum, the exercise must validate the list of partner agencies, the accuracy of the local communications matrix, and provide an assessment of the timeliness and effectiveness of communication processes.

CHAPTER 10 MARITIME PUBLIC BROADCAST OPERATIONS

A. General. Communication with the maritime public is required for prosecution of CG statutory missions. Generally, these communications include, but are not necessarily limited to SAR communication (addressed in Chapter 11 of this Manual) and broadcast of maritime safety information (MSI). Per 33 C.F.R. 72.01-25, the CG issues broadcast notice to mariners (BNM). Distress, urgent, and safety broadcasts are made as required, along with other regularly scheduled MSI broadcasts. A BNM is the method to disseminate important navigation safety information. In general, BNMs and regularly scheduled broadcasts include information vital to the maritime community operating in or approaching the coastal waters of the U.S., including Alaska, Hawaii, Guam, the Caribbean, and the high seas. Per Memorandum of Agreement (MOA), the CG cooperates with the National Oceanic and Atmospheric Administration/National Weather Service (NOAA/NWS) through radio broadcast of MSI, including weather and ice information, to mariners operating in coastal waters and on the high seas.

B. U.S. Coast Guard (CG)-National Weather Service (NWS) Coordination-Liaison Working Group (UNCLOG). The UNCLOG is a CG, NOAA/NWS, National Geospatial Intelligence Agency (NGA) working group established to administer and carry out the terms of the MOA discussed in the previous paragraph. UNCLOG responsibilities include configuration management of NOAA/NWS text and graphic products to be broadcast by CG communication facilities. Requests for new products or schedule changes that do not conform with UNCLOG established criteria as provided by the Area and Communications Command UNCLOG representatives must be submitted to Commandant (CG-672) for approval.

C. Maritime Safety Information (MSI). Maritime safety information (MSI) is information that is broadcast to mariners such as weather warnings and other dangers to navigation. Through U.S. participation in the United Nations (UN) IMO and the SOLAS Convention (EO 12234), the CG is responsible for disseminating MSI to mariners.

1. Broadcast Notice to Mariners (BNM). A BNM is the method by which important navigation safety information is disseminated. In general, these broadcasts include information vital to the maritime community operating in or approaching the coastal waters of the U.S., including Alaska, Hawaii, Guam, and the Caribbean. Record message formatting requirements for BNM of any type are included in Reference (r).

    a. Urgent Marine Information Broadcast (UMIB). Urgent broadcasts must be used to announce severe weather and issues regarding safety of life at sea (e.g., hurricanes, hurricane force winds, tsunami warnings).

    b. Safety Marine Information Broadcast (SMIB). The safety signal must precede a safety broadcast. Safety broadcasts must be made only when the information is so important to the safety of navigation that a delay in its dissemination would create a hazard to shipping. Each safety broadcast must normally consist of only one subject.

c. Scheduled Broadcast Notice to Mariners. Safety and urgent record messages that remain in effect at the next scheduled broadcast must be repeated.

(1) Area and District commanders must coordinate their broadcast times to minimize interference problems.

(2) HF and VHF-FM broadcasts must be scheduled so that interference does not occur in overlapping coverage areas.

(3) Area Commanders must publish scheduled BNM content and broadcast times for each broadcast station in their Annex K to Area OPLAN. Any proposed changes must be submitted through the Area C4IT division or District communications office.

2. Weather Warnings. Weather warnings are transmitted upon receipt as a safety broadcast from designated VHF-FM sites (see Appendix C).

a. Proposed changes to this list must be submitted through the District communications office and Area C4IT division to Commandant (CG-672), for consideration by the UNCLOG. An example of such a proposed change is the elimination of a CG broadcast where existing R21 RFFs are located in areas that SOLAS vessels do not transit and NOAA Weather Radio broadcast facilities overlap coverage with the R21 RFFs.

b. Area Commanders and the COMMCOM must designate an UNCLOG representative.

c. The area commander may modify or suspend the broadcast schedule during an emergency or where operational responsibilities dictate. Notification must be made to the UNCLOG by the Area UNCLOG representative.

3. Navigational Warnings. The CG keeps mariners aware of important safety information such as changes to aids to navigation, hazards, channel depths and conditions, and corrective information for charts and publications via navigational warnings. Navigation information is primarily disseminated in the form of Local Notices to Mariners, Light Lists, and BNMs. The BNM must be broadcast per the instructions contained in the record message. Cutters requiring this navigational information via record message must contact the applicable District (dpw), Sector, or District Command Center for guidance.

4. Broadcast Operations.

a. Urgent information and other warnings can be broadcast on international distress and calling frequencies (VHF-FM Channel 16 (156.800 MHz)) provided the broadcast does not exceed one minute.

b. An appropriate working frequency must be used for broadcasts requiring more time for transmission.

c. Units conducting broadcasts must avoid the practice of a single operator broadcasting live while simultaneously monitoring SAR frequencies. The requirement to conduct a broadcast does not relieve the unit of the requirement to sustain uninterrupted SAR frequency monitoring.

d. Radiotelephone broadcasts must be made at a normal conversational speed, but with the more important and more difficult portions (e.g., geographic coordinates, forecast winds) sent at reduced rate/speed to enable listeners to copy this information. Proper diction is essential and the text must be read in phrases rather than word by word. See paragraph D. of this Chapter, Broadcast Quality Control Monitoring Program.

e. Every effort must be made to ensure scheduled broadcasts start on time and do not exceed authorized time periods.

5. Broadcast Notice to Mariners (BNM) Originator Responsibilities.

a. The BNM originator must use the subject lines and readily recognizable abbreviations per Reference (r);

b. All BNMs must use Coordinated Universal Time (UTC) as the time of origination. Local time may also be placed in parenthesis in the text of the broadcast at unit discretion;

c. The length of record messages for the BNM broadcast must be kept to a minimum consistent with the need to pass important information;

d. To use the NAVTEX system as a broadcast alternative, BNM originators must ensure all types of broadcasts are formatted per Reference (r) to alleviate the need to re-key the NAVTEX transmission. An exception to this, if broadcasting NWS information, operators must transmit the exact text received from the NWS;

e. Originators of broadcasts must review their active BNMs daily, including broadcasts made by the NGA at CG request, to avoid transmitting duplicate or outdated information;

f. The originator must ensure broadcast record messages are cancelled once action is no longer necessary. Originators must provide a cancellation date on BNMs where possible. If no cancellation date is included on the BNM, the originator must send a cancellation record message;

g. Originators must issue weekly summaries of all active BNMs per Reference (r). Additional guidance is also available in Reference (a).

TYPE	VHF-FM Channel 16 (156.800 MHz)	VHF-FM Voice Working Channel 22 (157.1 MHz)	Distress NBDP NAVTEX 518 kHz
Scheduled Broadcasts	As scheduled	As scheduled	As scheduled
Safety Broadcast	Preliminary Announcement (Note 2)	A C F	C E F IMPORTANT
Urgent Broadcast	Preliminary Announcement (Note 1,2)	A B D F	E D F VITAL
Urgent Cancellation	Preliminary Announcement (Note 1)	A	E VITAL

A: Upon receipt,

B: Every 15 minutes for a 1 hour period.

C: Repeat next scheduled broadcast, unless cancelled.

D: Repeat on scheduled broadcasts until cancelled.

E: At first available period after receipt when frequency not in use.

F: Additional broadcasts as directed by originator.

Note 1: Broadcast on VHF-FM Channel 16 (156.800 MHz) if less than one minute long. Otherwise broadcast on working frequency.

Note 2: Preliminary announcement on Distress frequency - Continue on working frequency.

Figure 10 - Radiotelephone and NAVTEX Broadcast Requirements

6. Broadcast Service Changes and Casualties. The CG must notify the maritime community of changes or outages in distress, safety, and broadcast operations. The following section provides further policy on service changes and casualties.

   a. Changes, casualties, and casualty corrections concerning the following services must be sent to the applicable CG broadcast station for broadcast as a BNM:

      (1) VHF-FM Channel 16 (156.800 MHz) watch-keeping;

      (2) VHF-FM Channel 22A (157.100 MHz);

      (3) District CC and SCC emergency telephone; and,

      (4) HF/VHF DSC capabilities.

   b. Changes, casualties, and casualty corrections concerning the following broadcast station services must be via CGFIXIT ticket and sent to COGARD COMMCOM VA and NGA NAVSAFETY WASHINGTON DC for broadcast to navigational area (NAVAREA) IV (Atlantic), NAVAREA XII (Pacific), HYDROPAC, or HYDROLANT Navigation Warning:

      (1) NAVTEX broadcasts;

      (2) HF SITOR, HF voice, and HF Radiofax (ice and weather) broadcasts;

      (3) HF Single sideband voice GMDSS guards; and,

      (4) Area CC emergency telephone and telex numbers.

   c. For outages that impact District and Area CCs, the following must be notified:

      (1) Vizada Southbury, CT Teleport: (203) 262-5010

      (2) Inmarsat London UK: 011-44-0-20-7728-1142

   d. In addition to broadcasts, changes or casualties to services or capabilities expected to last more than seven days must be published and posted via BNM, with anticipated date of service restoral.

7. Navigational Telex (NAVTEX).

   a. Description. NAVTEX is a system for broadcasting BNMs, weather warnings and forecasts, ice warnings, and other marine information by automatic printout using the internationally designated frequency 518 kHz. NAVTEX receivers are used on merchant and passenger vessels, offshore fishing vessels, and pleasure vessels. Messages for broadcast over NAVTEX must be formatted as a BNM per Reference (r). In addition;

      (1) NAVTEX is a service specifically designed for the promulgation of maritime safety information as a part of the GMDSS. All SOLAS-regulated ships are required to carry NAVTEX receivers. NAVTEX coverage generally extends to 200 nautical miles off the coast.

      (2) CG CCs use this broadcast method to alert ships in those coastal areas covered by NAVTEX of SAR and SAR-related information.

(3) The Commander, International Ice Patrol uses this system as a means of disseminating ice bulletins and warning messages.

(4) Districts, Sectors, and NAVCEN use this system as a means of disseminating BNMs.

b. Administration. NAVTEX policy is administered by the IMO's International NAVTEX Coordinating Panel. Commandant (CG-672) is the national NAVTEX coordinator. Area Commanders are the NAVTEX coordinators for the CG, and must ensure broadcasts are reliable, on schedule, within the prescribed duration, and practicable without interference.

c. Operational Requirements. The IMO publishes NAVTEX operational requirements in its Safety of Life at Sea Convention (SOLAS), which is a treaty document in the United States.

d. Priority Message Handling. The three NAVTEX message priorities, in descending order of urgency, used to dictate the timing of the first broadcast of a new warning are as follows:

(1) Vital. For immediate broadcast. Corresponds to an urgent broadcast, generally applying only to SAR, hurricane, hurricane force winds, or tsunami related messages. Broadcasts of lower priority in progress must be stopped if possible to permit transmission of vital messages.

(2) Important. For broadcast at the next available period when the frequency is unused. Corresponds to a safety broadcast (i.e., broadcast upon receipt, then at scheduled broadcasts).

(3) Routine. For broadcast at the next scheduled transmission. Corresponds to a scheduled broadcast (i.e., broadcast at next scheduled broadcast, no safety broadcast required).

e. Broadcast Schedule.

(1) CG NAVTEX broadcasts are conducted IAW Figure 10 as scheduled in Figures 11 and 12.

(2) All broadcasts have navigational warnings, if required.

(3) BNMs. Broadcasts may exceed this 40 minute limit if there is no other station in the area scheduled for that period, or if the station scheduled for that period gives permission to continue broadcasting.

(4) If broadcast is expected to exceed 40 minutes, all new messages must be transmitted during the first 40 minutes.

(5) BNMs must be broadcasted for the period designated by the originator.

(6) Repeats of BNMs must be moved to the two daily broadcast slots where weather is not normally broadcast.

(7) Although IMO limits NAVTEX broadcast duration to 10 minutes, the CG is authorized a 20 minute transmit duration due to greater than normal site separation in the U.S. The maximum duration of a NAVTEX broadcast is 40 minut

(8) If permission to exceed 40 minutes is not granted via COMMCOM, then messages not transmitted must be broadcast during the next period, immediately after all urgent and new messages, but before repeated messages.

f. Broadcast messages are sent as follows:

(1) Messages are sent in the order received and in order of message priority.

(2) Newer messages received must be transmitted first before other messages received.

(3) Messages broadcast during the previous schedule must be broadcast at the end of the broadcast.

f. Warnings are normally repeated at every scheduled transmission for as long as they remain in force. Negative tidal surge and tsunami warnings are normally the subject of navigational warnings, broadcast upon receipt, and at subsequent scheduled transmissions.

(1) Navigational warnings broadcast on NAVTEX normally include District BNMs and other information designated by the District.

(2) NAVTEX does not include local warnings, detailed information on aspects that the oceangoing ship normally does not require, or warnings originated by the NGA NAVAREA, HYDROLANT, or HYDROPAC.

g. Messages cancelled by a cancellation message must be removed from the broadcast after the cancellation message broadcasts (along with the cancellation message).

h. The forward error correction idle signal must be transmitted between each NAVTEX message to allow NAVTEX receivers to re-synchronize.

i. Means must be provided for the reduction of transmission power at night if interference is caused to other stations.

j. NAVTEX required time of scheduled broadcast is as follows:

Broadcast Station	Identifier	Broadcast Schedule (UTC)
RCF Boston	F	0050, 0450, 0850*, 1250, 1650, 2050*
COMMCOM Chesapeake, RCF Pungo	N	0210*, 0610, 1010, 1410*, 1810, 2210
RCF Charleston	E	0040, 0440, 0840*, 1240, 1640, 2040*
RCF Miami	A	0000, 0400, 0800*, 1200, 1600, 2000*
RCF New Orleans	G	0100, 0500, 0900*, 1300, 1700, 2100*
Sector San Juan	R	0250*, 0650, 1050, 1450*, 1850, 2250
(*) Weather is normally broadcast four times per day. This symbol annotates the times when weather is not broadcast.		

Figure 11 - Atlantic Area NAVTEX Broadcast Schedules

Broadcast Station	Identifier	Broadcast Schedule (UTC)
COMMDET Kodiak(East)	J	0130, 0530, 0930*, 1330, 1730, 2130*
COMMDET Kodiak(West)	X	0350, 0750, 1150*, 1550, 1950, 2350*
RCF Astoria	W	0340*, 0740, 1140, 1540*, 1940, 2340
RCF Pt. Reyes/San Francisco	C	0020, 0420*, 0820, 1220, 1620*, 2020
RCF Cambria	Q	0240*, 0640, 1040, 1440*, 1840, 2240
RCF Honolulu	O	0220, 0620, 1020*, 1420, 1820, 2220*
Sector Guam	V	0330, 0730, 1130, 1530, 1930, 2330
(*) Weather is normally broadcast four times per day. This symbol annotates the times when weather is not broadcast.		

Figure 12 - Pacific Area NAVTEX Broadcast Schedule (UTC)

8. Additional Automated Broadcast Systems. Certain HF broadcast functions are automated through software application at COMMCOM and keyed from the Remote Communications Facilities (RCFs) and COMMDET Kodiak. These automated functions help assure broadcast schedules are met and that broadcasts are conducted consistently for high seas mariners. Frequency assignment and broadcast schedules are found in Annex K to Area OPLAN.

   a. Voice Broadcast Automation (VOBRA). Voice Broadcast Automation (VOBRA). VOBRA are CG HF voice broadcasts performed in the upper sideband mode using a synthesized voice known as "Iron Mike". VOBRA provides computer-controlled, voice-synthesized weather broadcasts on HF at regularly scheduled times and ensures all voice broadcasts are conducted at consistent speed and diction for maximum intelligibility and as an aid for identifying and copying these weather broadcasts. VOBRA are broadcast by the COMMCOM and Sector Guam. The current broadcast schedule is found in Appendix C of this Manual.

   b. Simplex Teletype Over Radio (SITOR). SITOR is used to broadcast marine safety information including high seas forecasts, NAVAREA warnings, ice, and hydrographic information in hard copy form. CG SITOR (Simplex Teletype Over Radio) text broadcasts are performed in mode B, FEC. SITOR is also known as Narrow Band Direct Printing (NBDP). SITOR/NBDP is an automated direct printing service similar to NAVTEX but does not offer all of the same functionality such as avoiding repeated messages. SITOR is broadcast via RCF Boston, RCF Pt. Reyes, RCF Honolulu, and Sector Guam. The current broadcast schedule is found in Appendix C of this Manual.

   c. Radio Facsimile (Radiofax). Radiofax is an automated service provided by the National Weather Service. The National Weather Service Radiofax program prepares high seas weather maps for broadcast via RCF Boston, RCF New Orleans, RCF Pt. Reyes, COMMDET Kodiak, and RCF Honolulu transmitter sites. These broadcasts are prepared by the Ocean Prediction Center, National Hurricane Center, Honolulu Forecast Office, and Anchorage Forecast Office. Limited satellite imagery, sea surface temperature maps, and text forecasts are also available. Radiofax products are traditional weather charts for specific geographic areas.

   d. Inmarsat SafetyNET. SafetyNET is a service of Inmarsat’s Enhanced Group Call (EGC) system and was specifically designed for promulgation of maritime safety information as a part of GMDSS. Shore-to-ship distress and search and rescue broadcasts can be made at no charge to all Inmarsat equipped ships in a particular Inmarsat ocean region. Broadcasts must be limited to those cases involving grave and imminent danger. See Chapter 11, paragraph G.4.c., for additional discussion on the use of SafetyNET for SAR.

D. Broadcast Quality Control Monitoring Program. The following section provides policy for the Broadcast Quality Control Monitoring Program.

1. Program Description.

   a. Area Commanders must establish a monitoring and customer feedback program for all BNMs (e.g., 800 numbers, internet web pages) with the goal of improving BNM communication procedures.

   b. Area Commanders must engage the CG Auxiliary where appropriate to assist in these efforts. This engagement must be initiated and managed through the Auxiliary Department of Operations communications Division at the national level (AUX-DVC-OT) who must designate an Auxiliary command point of contact for the COMMCOM.

   c. All communication facilities making BNMs must establish a program to review the broadcast for content, format, broadcast time, proper frequency, and antenna selection (to reach the desired area of geographic coverage). "Service to the mariner" must be the guiding principle in this review. Suggestions for improvements in content or format must be submitted to the originating agency. Suggestions for changes in broadcast time or frequencies must be submitted to the UNCLOG via the chain-of-command. (see paragraph B of this Chapter for UNCLOG description).

      (1) NAVTEX, HF SITOR, HF Radiofax, SafetyNET, and HF voice broadcasts must be monitored for broadcast assurance and quality by the COMMCOM; and,

      (2) All Sectors must monitor their broadcasts for quality on a random basis at least weekly.

   d. In addition, commanding officers of units that broadcast MSI must work with the regional Base C4IT department to measure transmitter performance. Such measurements must include measurement and verification of transmitted power, voltage standing-wave ratio, carrier frequency, and where applicable mark/space tone placement, frequencies, and tolerances.

2. Broadcast Quality Control Elements. The following elements are evaluated during the monitoring process:

   a. Transmission quality, particularly the communication procedures;

   b. Product quality, formats, and content; and,

   c. Availability to the user to the extent practicable (e.g., the schedule and the geographic coverage which is dependent primarily on the frequencies and antennas used for the broadcast).

CHAPTER 11 SEARCH AND RESCUE (SAR) COMMUNICATIONS

A. General. A primary function performed by CG communication personnel is to provide rapid and reliable communication to vessels in distress. The objective of SAR communication is to obtain information on a distress incident and disseminate it promptly to all units and commands capable of providing assistance. Coordination of participants during the SAR operation is necessary to save lives and property involved. Communication procedures relative to distress and those pertaining to the use of the distress, urgency, and safety signals are found in Articles 30 through 34 of the ITU Radio Regulations.

1. Under 14 U.S.C § 102(3) the CG must develop, establish, maintain, and operate rescue facilities for the promotion of safety of life and property on and under the high seas and waters subject to the jurisdiction of the U.S. covering all matters not specifically delegated by law to some other executive department; and
2. CG personnel involved with SAR responsibilities must adhere to current procedures described in Reference (d), Communications Instructions Distress and Rescue Procedures, ACP 135 (series), and ITU Radio Regulations.

B. Coast Guard (CG) Search and Rescue (SAR) Organization and Responsibilities.

1. Rescue Coordination Center (RCC) and Command Center (CC). RCC and CC responsibilities and geographic locations can be found in Reference (d). The RCC function is performed at the District CC, and the SAR mission coordinator (SMC) role is performed at both the District CC and the Sector CC levels.
2. Coordination of Search and Rescue (SAR) Communication. The coordination of communication relating to SAR incidents closely follows the command structure of the SAR case. All communications destined for the cognizant RCC or CC must be via the on-scene coordinator. Procedures for coordinating SAR communication are in Reference (a).
3. Distress Communication Responsibilities. Area and District Commanders must organize the communication facilities in their AOR, and must provide detailed instructions for the correct procedure for reporting and broadcasting distress information. In addition, Area and District Commanders must ensure:
   a. Assignment of continuous radio watches on distress frequencies by as many units as necessary to provide adequate AOR coverage. See Chapter 5 of this Manual for specific frequency guard requirements for CG shore facilities, vessels, and aircraft;
   b. All units proactively respond to all distress calls received and ensure the call is relayed to the appropriate RCC/Sector CC; and,
   c. Prompt broadcast of distress information, per current laws and privacy policies, to the maritime public who may be capable of providing assistance.
      (1) The CG frequently intercepts communication from masters to owners reporting their vessels disabled, aground, or in a condition that indicates the possible need for assistance. The CG must evaluate this information to determine if the situation merits a distress or non-distress situation. This information must not be released for publication.

(2) Refer public requests for the release of any recorded audio or logs to the unit's servicing legal office.

C. Distress Communication Policy.

1. Distress Call and Message. Distress traffic consists of all messages relating to the immediate assistance required by a ship or aircraft in distress, including SAR communication and on-scene communication. The distress call and message has priority over all other transmissions or traffic.

   a. All stations that hear or receive a distress call or message must immediately cease transmission and continue to listen on the frequency used for the transmission of the distress until satisfied that assistance is being rendered;

   b. No transmissions must interfere with distress traffic;

   c. Since a distress call is not addressed to a particular station, an acknowledgment of receipt must not be given until the distress call is completed.

2. Medical Communication (MEDICO). MEDICOs and medical evacuations are part of the traditional CG SAR mission. All MEDICO messages are a potential assistance case and of interest to the CG. The CG is not acting as a government agency responsible for providing free medical message service. Instead, the CG radio facilities are used free of charge in the same manner as commercial facilities for this type of service. National Geospatial- Intelligence Agency's Radio Navigational Aids, Pub 117 (series) and ITU's "List of Coast Stations and Special Service Stations (List IV)" contain commercial and government radio stations that provide free medical message services to ships. Deadhead (DH) MEDICO (non-chargeable medical message) message procedures are contained in Reference (a).

   a. The CG accepts DH MEDICO messages and must deliver them to the appropriate Area or District CC;

   b. The CG must deliver messages requesting medical advice to hospitals or other facilities where authorities or the communication facility involved has made prior arrangements. RCCs and Sector CCs must establish procedures for consultation with medical facilities or CG assigned Public Health Service medical doctors;

   c. Area CCs must have local procedures in place for handling incorrectly addressed DH MEDICO messages;

   d. In the event a medical case develops a need for CG assistance, the messages must be handled by CG units when possible. In most cases, the CG must not assume any charges for DH MEDICO messages. Where it is not possible to use CG units, and there is a need for CG assistance, the CC must send a DH MEDICO message chargeable to the CG via commercial facilities;

   e. CCs must maintain liaison with commercial facilities to ensure the CG remains well informed regarding MEDICO messages not handled via CG circuits.

3. Medical Communication. For the purpose of announcing and identifying medical transports protected under the 1949 Geneva Conventions and additional protocols, the procedures for urgency broadcast must be followed, with the urgency signal followed by the single word 'MEDICAL' (pronounced MAY-DEE-CAL).

4. Initial Search and Rescue (SAR) Check Sheet. Communication watchstanders must use an initial SAR check sheet, per Reference (c), for all SAR related reports. An example of an initial SAR check sheet is contained in Reference (c).
5. Distress Electronic Mail (Email) and Text Messaging Policy. Email and text messaging are not designed for distress communication; therefore, the CG does not encourage use of either service for distress alerting purposes. Additional information regarding distress Email and text messaging is contained in Reference (c).
6. Telephone Policy. The commanding officer or officer-in-charge of each unit must ensure personnel are proficient in handling telephone calls of a distress nature before assigning them to duty answering telephones. In addition, if the CG unit cannot take action in response to a distress call, the commanding officer or officer-in-charge must ensure personnel know how to relay the information to the appropriate authority.
7. Distress Cellular Telephone Policy. Marine cellular telephone usage is widespread, and an increasing number of boaters are relying on cellular telephones in conjunction with, or instead of, VHF-FM radio.
    a. A voice call made via cellular telephone will be recorded on the Sector CC's DVL as long as the call is made to a distress telephone line. When properly used, cellular telephones meet the requirements of reliable communication as outlined in Reference (c). Cellular telephone communications are point-to-point. Cellular telephone conversations cannot be heard by other boaters in the area who may be in a position to render immediate aid to someone in distress.
    b. When a distress call is received via cellular telephone and the caller's location is not known, use the procedures outlined in References (a) and (c) to determine the location of the caller.

D. Rescue 21 (RESCUE 21) Direction Finding (DF) Monitoring.
1. The RESCUE 21 Guard receiver at each RESCUE 21 Remote Fixed Facility (RFF), if installed, is permanently tuned to VHF-FM Channel 16 (156.800 MHz).
2. The RESCUE 21 DF receiver must remain tuned to VHF-FM Channel 70 DSC (156.525 MHz) unless temporarily tuned to a different VHF-FM working channel to meet other operational needs.

E. Auto-Distress Communications. Auto-distress transmissions are often triggered accidentally, creating potentially dangerous safety of life issues for the public and the CG. Morse code S-O-S transmissions and automated/ synthesized voice MAYDAY broadcasts on Channel 16 VHF-FM are transmitted without position or vessel identification and must be responded to per Reference (c).

F. Global Maritime Distress and Safety System (GMDSS). GMDSS is an international system that uses terrestrial and satellite technology, along with shipboard radio systems, to ensure rapid, automated alerting of shore-based communication and rescue authorities in addition to ships in the immediate vicinity for maritime distress events.

1. Applicability to Commercial Vessels. GMDSS equipment requirements are mandatory for vessels subject to the Safety of Life at Sea (SOLAS) Convention of 1974, as amended. In addition, U.S. ships subject to Title II, Part II and Part III of the Communications Act of 1934, as amended, have to carry GMDSS equipment under FCC Regulation 47 C.F.R. Part 80 Subpart W. These include all ships, including fishing vessels, to be navigated in the open sea outside of a harbor or port, except: DSC

   a. Ships other than passenger vessels less than 300 gross tonnage;

   b. Passenger ships having six passengers or less;

   c. U.S. government ships;

   d. Yachts of less than 600 gross tons;

   e. Vessels in tow;

   f. Ships navigating solely on any bays, sounds, rivers or protected waters within the U.S.;

   g. Ships navigating within the Great Lakes of North America; and,

   h. Small passenger ships meeting the requirements of 47 C.F.R. Part 80 Subpart S.

2. Global Maritime Distress and Safety System (GMDSS) Coverage Areas. GMDSS divides the world's oceans into four sea areas. SOLAS ships have distinct equipment carriage requirements for each area through which they transit:

   a. Sea Area A1. An area within the radiotelephone coverage of at least one VHF-FM coast station in which continuous DSC (VHF-FM Channel 70 (156.525 MHz)) alerting and VHF-FM Channel 16 (156.800 MHz) radiotelephony services are available, as defined by the IMO. Sea area A1 covers the area from the coastal area up to approximately 20 nautical miles offshore;

   b. Sea Area A2. An area within the radiotelephone coverage of at least one MF coast station (excluding sea area Al) in which continuous DSC (2187.5 kHz) alerting and 2182 kHz radiotelephony services are available, as defined by the IMO. GMDSS-regulated ships traveling this area must carry a DSC-equipped MF radiotelephone in addition to equipment required for sea area A1. Sea area A2 covers the area from the coastal area up to approximately 200 nautical miles offshore;

   c. Sea Area A3. An area within the coverage area of a recognized GMDSS mobile satellite service (excluding sea areas A1 and A2) in which continuous alerting is available. Ships traveling this area must carry a ship earth station or a DSC-equipped HF radiotelephone/telex, in addition to equipment required for sea areas A1 and A2. Sea area A3 covers the area between roughly 70º North and 70º South;

   d. Sea Area A4. The remaining sea areas outside sea areas A1, A2, and A3 (i.e., Polar Regions). Ships traveling this area must carry a DSC-equipped HF radiotelephone/telex, in addition to equipment required for sea areas A1, A2, and A3.

3. Distress Alerting Methods. The 406 MHz Emergency Position Indicating Radio Beacon (EPIRB) and Inmarsat C and Iridium short data distress alert are the internationally recognized methods of satellite distress alerting under GMDSS. DSC is the internationally recognized method of sending a digital distress alert. For mariners not equipped with EPIRBs, or DSC, traditional MF, HF, and VHF-FM distress voice channels are the preferred methods of distress alerting.
4. Additional GMDSS Policy.
   a. Harmful Interference. Any emission causing harmful interference to distress and safety communication on any of the discreet GMDSS frequencies is prohibited. Before transmitting on a GMDSS frequency for any purpose other than distress, a station must listen on the frequency to ensure no distress transmission is being sent.
   b. Test Transmissions. For GMDSS frequencies, the number and duration of test transmissions must be kept to a minimum. Test transmissions must be coordinated with a competent authority, and carried out on artificial antennas or with reduced power when possible. For distress and safety calling frequencies, test transmissions should be avoided; however, if unavoidable, a test transmission announcement must be made on that frequency.
   c. CG Survival Craft. Radiotelephone equipment installed in survival craft that operates in the frequency range of 156 MHz to 174 MHz must have the capability to transmit and receive on VHF-FM Channel 16 (156.800 MHz) and at least one other frequency in that range.
   d. Distress Traffic. Distress traffic consists of all messages relating to the immediate assistance required by the ship in distress, including search and rescue communication and on-scene communication. For distress traffic by radiotelephony procedures, refer to Reference (a).
      (1) Error correction techniques must be used for distress traffic by direct-printing telegraphy. Distress communication by direct-printing telegraphy should normally be established by the ship in distress and should be in the broadcast mode of forward error correction (FEC). If advantageous, the automatic repeat request (ARQ) mode may subsequently be used.
      (2) The RCC/CC responsible for coordinating SAR operations must manage distress traffic relating to the incident or appoint this responsibility to another station.
         (a) If a station interferes with distress traffic, silence can be imposed by the RCC coordinating distress traffic, the unit coordinating SAR operations, or the coast station involved with the distress. Silence imposition can be addressed to all stations or to a single station. In narrow-band direct-printing telegraphy, silence is imposed normally using FEC mode through the SILENCE MAYDAY signal. However, the ARQ mode may be used when it is advantageous to do so; and,
         (b) When the distress situation concludes, the CC controlling a SAR operation must initiate a message for transmission on the distress traffic frequencies indicating the distress traffic has ceased.

(3) On-scene communication. On-scene communication is defined as: (1) the communication between the vessel in distress and the assisting response unit(s), and (2) the communication between the response unit(s) and the unit coordinating SAR operations. The unit coordinating SAR operations must have control of on-scene communications.

(4) Inmarsat and Iridium are recognized mobile satellite service providers of GMDSS and may not charge for distress communications.

e. Maritime Mobile Service Identity (MMSI) Numbers. The IMO adopted the ITU MMSI as an internationally recognized method mainly for identifying AIS and DSC transmissions. MMSIs are regulated and managed internationally by the ITU, just as radio call signs are regulated. The MMSI format and use is documented in Article 19 of ITU Radio Regulations and ITU-R Recommendation M.585 (series). See Chapter 4, Paragraph D.1. of this Manual for information on assignment and maintenance of MMSI for CG radios.

f. Maritime Mobile Service Identity (MMSI) Search and Rescue (SAR) Vessel Identification System. The MMSI Vessel Identification System is a web-based application managed by the C5ISC. Access to this data will help identify vessel ownership history, state registered vessels that change registration to other states, and changes in law enforcement status for vessels.

G. Global Maritime Distress and Safety System (GMDSS) Sub-Systems. GMDSS consists of numerous communication sub-systems, including:

1. Digital Selective Calling (DSC). Used for distress, urgency, safety, routine, ships business, and test calling via HF and VHF-FM. DSC is digital technology intended to initiate non-voice communication over maritime radio and provide distress alert information to CG RCCs/CCs and foreign RCCs. Vessels subject to the Safety of Life at Sea (SOLAS) Convention do not stand an open speaker watch on MF/HF and only respond to DSC calls.

a. General Digital Selective Calling (DSC) ITU Requirements.

(1) Ship-to-ship distress alerts are used to alert other ships in the vicinity of the ship in distress and are based on the use of HF and VHF bands.

(2) A station in the mobile maritime or mobile-satellite service must initiate and transmit a distress alert relay for a vessel that is unable to transmit a distress alert. The station transmitting the distress alert relay must indicate it is not the vessel in distress.

(3) Coast stations and appropriate land earth stations that receive distress alerts must route the alert as soon as possible to the RCC.

(4) Radiotelephone distress acknowledgement responsibilities can be found in Reference (s).

b. Digital Selective Calling (DSC) Categories. DSC calls fall into the following categories: distress, urgency, safety, and routine. Important information to be obtained from an incoming DSC call is the category of call, the MMSI number, information for following up with voice communication, and (for distress calls) the position and nature of distress.

c. CG General DSC Policies:

(1) DSC All-Ships urgent or safety priority calls must be made on VHF-FM only. On MF/HF, an urgent or safety call must be addressed to a specific ship or to a specified geographical area. An All-Ships call is not permitted on MF/HF.

(2) The follow-on voice frequency/channel identification must be included in the alert, and must be the voice working frequency/channel corresponding to the selected DSC frequency.

(3) Once the DSC alert is sent, a transceiver must be changed to the corresponding voice frequency and the follow-on voice announcement must be made.

(4) The ITU Sector for Radio Communications indicates excessive test calls on MF/HF DSC distress and safety frequencies are overloading the system to the point where they are interfering with distress and safety calls. To minimize possible interference, testing with coast stations must be kept to a minimum.

(5) DSC distress calls are electronically relayed to the CG by any vessel with a DSC compatible radio.

(6) DSC calls use the applicable MMSI number and appropriate DSC guard or calling frequencies. Mariners can instantly send an automatically formatted distress alert to the CG or other rescue authority anywhere in the world.

(7) Mariners can initiate or receive distress, urgency, safety, and routine radiotelephone calls to or from any similarly equipped vessel or shore station.

(8) Users may call a specific station, group of stations, or all stations to establish communications.

d. CG Shore Unit DSC Response Policy. Shore units receiving DSC distress alerts must first acknowledge receipt of the call via DSC and then attempt to establish voice communication on an appropriate channel. RCC/CC personnel must attempt to identify the vessel, either through database sources or by contacting the appropriate foreign RCC based on the country code of the caller's MMSI (i.e., the first 3 digits). There are no restrictions on CC personnel contacting foreign RCCs for the purposes of SAR operations.

(1) The RESCUE 21 system provides CG Sectors with VHF-FM DSC capability.

(2) VHF-FM radios equipped with DSC maintain a continuous radio guard on VHF-FM Channel 70 (156.525 MHz), regardless of the channel selected manually on the front panel. When a DSC distress alert is received on VHF-FM Channel 70 (156.525 MHz), most of these radios will emit a loud audio alarm and the radio will automatically shift to VHF-FM Channel 16 (156.800 MHz). If the radio does not automatically shift to VHF-FM Channel 16 (156.800 MHz) then the operator must manually shift the radio.

(3) VHF-FM DSC distress alerts must be considered the equivalent of a MAYDAY distress alert, and require the same level of response per Reference (c).

e. CG Vessel DSC Response Policy. CG vessels equipped with VHF-FM DSC equipment must ensure these radios maintain a continuous radio guard on VHF-FM Channel 70 (156.525 MHz), regardless of the channel selected manually on the front panel.

(1) When a DSC distress alert is received on VHF-FM Channel 70 (156.525 MHz), the radio will emit a loud audio alarm. This alarm is the equivalent of a MAYDAY and must be handled with the same level of response. The radio should automatically shift to VHF-FM Channel 16 (156.800 MHz), but if the automatic shift does not occur, operators must manually shift channels.

(2) As soon as possible, the SAR mission coordinator (SMC)/commanding office/officer-in charge (whichever is applicable for the CG vessel reporting requirements) must be informed of the contents of the distress alert.

(3) In areas where reliable VHF-FM DSC communications with one or more shore stations are known not to exist, CG vessels that receive a VHF-FM DSC distress alert must, as soon as possible, notify the appropriate SCC and acknowledge receipt of the distress alert when instructed.

(4) In areas where reliable VHF-FM DSC communications with one or more shore stations are feasible, the commanding office/officer-in-charge must defer acknowledgement so that a shore station can acknowledge receipt of a call. Any CG vessel receiving a call that is not acknowledged by a shore station within one minute must acknowledge the call using the following policy:

(a) Acknowledge receipt of the alert on VHF-FM DSC and attempt to establish communication with the distressed vessel on VHF-FM Channel 16 (156.800 MHz);

(b) If unable to establish voice communication with the distressed vessel, CG vessels must acknowledge receipt of the distress alert using the DSC acknowledgement function on the DSC transceiver. This action will send a DSC acknowledgement message to the distressed vessel, terminate the DSC distress call, and cause that radio to shift to VHF Channel 16 (156.800 MHz). A follow on call on VHF Channel 16 (156.800 MHz) must be made to the distressed vessel to establish voice communications; and,

(c) CG vessels that acknowledge receipt of DSC distress alerts must inform the applicable RCC and OPCON/TACON (if different) by the most expeditious means and provide relevant distressed vessel information (e.g., Maritime Mobile Service Identity (MMSI), position, nature of distress) obtained through the DSC alert.

f. High Frequency (HF) Digital Selective Calling (DSC) Response Policy. DSC is unique in that distress communication is initiated by widely distributed digital data bursts, but all follow-up communication after initial acknowledgement are typically handled on the associated voice frequency.

(1) ITU regulations require each unit that receives a DSC distress alert or distress relay to send an acknowledgment. DSC acknowledgment does not imply assumption of SMC by the acknowledging unit. Acknowledgement simply indicates that a shore unit has received the DSC distress alert and the CG is responding;

(2) Multiple units may respond to the DSC distress alert. It is critical that CG units communicate with one another and with the default SAR mission coordinator (SMC) to ensure role clarity during DSC case operations;

(3) Shore units receiving a DSC alert outside their area of responsibility must wait one minute to allow the responsible unit to acknowledge receipt of the distress. However, during this wait period, units hearing the distress must notify their operational commander/RCC and contact the Sector/unit closest to the distress to ensure they are aware of and are responding to the distress;

(4) Further information regarding SMC determination, delegation, and responsibilities are found in Reference (c).

(5) Digital Selective Calling (DSC) Guard Frequencies. DSC guard frequencies and their associated voice and SITOR frequencies are listed in Figure 13. Figure 14 lists the MF/HF DSC Alert Monitoring Schedule for COMMCOM, COMMDET Kodiak, and Sector Guam.

DSC Guard Frequency	Voice Frequency	SITOR Frequency
156.525 MHz[1]	156.800 MHz	N/A
4207.5 kHz	4125 kHz	4177.5 kHz
6312.0 kHz	6215 kHz	6268 kHz
8414.5 kHz	8291 kHz	8376.5 kHz
12577.0 kHz	12290 kHz	12520 kHz
16804.5 kHz	16420 kHz	16695 kHz

Figure 13 - Digital Selective Calling (DSC) Guard Frequencies, Associated Voice and SITOR Frequencies

[1] Very High Frequency-Frequency Modulation (VHF-FM) Channel 70 (156.525 MHz). This frequency is used in the maritime mobile service for digital selective calling, including DSC distress and safety calls. Use of this frequency for voice and communication other than DSC is prohibited.

DSC Alert Monitoring Schedule					
		Station and Schedule (UTC)			
kHz SHIP Station	**kHz Coast Station**	**NMF**	**NMN**	**NMA**	**NMG**
4125	**4125**	2300 - 1100Z	2300 - 1100Z	2300 - 1100Z	2300 - 1100Z
6215	**6215**	24 HRS	24 HRS	24 HRS	24 HRS
8291	**8291**	24 HRS	24 HRS	24 HRS	24 HRS
12290	**12290**	1100 - 2300Z	1100 - 2300Z	1100 - 2300Z	1100 - 2300Z
		Station and Schedule (UTC)			
kHz SHIP Station	**kHz Coast Station**	**NMC**	**NMO**	**NOJ**	**GUAM**
4125	**4125**	24 HRS	0600 - 1800Z	24 HRS	
6215	**6215**	24 HRS	24 HRS	24 HRS	0900 - 2100Z
8291	**8291**	24 HRS	24 HRS		
12290	**12290**	24 HRS	1800 - 1600Z		2100 - 0900Z
Note 1: 8291 and 12290 kHz are available under NOJ upon request					
Note 2: 16420 is available at all stations upon request					

Figure 14 - DSC Alert Monitoring Schedule

GMDSS Sub-Systems (continued).

2. Navigational Telex (NAVTEX). See Chapter 10 of this Manual for further information regarding NAVTEX broadcasts.
3. Simplex Teletype Over Radio (SITOR). SITOR is a long-range service for use in ship-to-shore and shore-to-ship communication as part of the GMDSS for maritime safety information, and can be used as an alternative to satellite communication. SITOR employs a forward error correction (FEC) mode of data for maritime safety broadcasts and automatic repeat request (ARQ) for other transmissions to minimize the effects of poor HF propagation conditions. See Chapter 10 of this Manual for further information regarding SITOR broadcasts.
4. Inmarsat. Virtually all navigable waters (less Polar Regions) of the world are covered by Inmarsat satellites. Inmarsat terminals provide telephone, data, facsimile, TELEX, Email, and videoconferencing capabilities. Inmarsat provides service access codes for medical advice and medical assistance. Inmarsat C is used for distress alerting, data communication, and reception of maritime safety information. The Inmarsat C system offers two way data communication. Some terminals have message preparation capabilities while others have ports to connect to a

personal computer. TELEX, Email, and distress messages similar to an EPIRB alert message can be sent from this type of terminal.

a. Distress messages directed to the CG are routed to the appropriate LANTAREA or PACAREA RCC/CC. Inmarsat C TELEX replies to ships sending distress alert messages are sent using distress priority.

b. District CCs have access to a web page established and maintained by the Inmarsat C provider. This web page allows CC personnel to send distress priority messages to the vessel, or vessels in the vicinity of the distressed vessel. If web or internet access is not available, a fax message can be sent to the desired land earth station for broadcast. CC personnel must call the satellite provider operator to verify receipt of fax. Inmarsat C numbers are recognized by a nine digit number beginning with "4."

c. SafetyNET is a service of Inmarsat's Enhanced Group Call (EGC) system and was specifically designed for promulgation of maritime safety information as a part of GMDSS. The EGC system provides an automatic, global method of broadcasting messages to all Inmarsat C GMDSS-equipped vessels in both fixed and variable geographical areas.

(1) CG RCC/CCs must disseminate and monitor SAR and distress related information using the Inmarsat SafetyNET system when the SAR case location is deemed to be outside the coverage of NAVTEX.

(2) CCs must not disseminate routine navigational information via SafetyNET.

(3) SafetyNET service is provided through the satellite provider's web interface, and via voice operator in case of internet failure, per Reference (d). SafetyNET message drafters should be aware of specific formatting required to ensure messages reach the targeted area. Charts of Inmarsat service areas are available on the CG NAVCEN website.

5. Radiotelephone. Radiotelephone is communication by voice radio. CG radiotelephone operators must be well trained and proficient, and as CG representatives, must always be professional. Military radiotelephone procedures are prescribed in Communication Instructions Radio Telephone Procedures, ACP 125 (series). All other radiotelephone procedures must be IAW Reference (s) and ITU Regulations. Area and District Commanders, commanders of logistics commands, and unit commanding officers must ensure all operational shore units under their control follow the procedures per the Communications Watchstander Qualification Guide, COMDTINST M16120.7 (series) and Reference (s) for preparing personnel for duties as communication watchstanders. The following is a list of common radiotelephone frequencies used by the CG for SAR communications (CG shore unit, vessel, and aircraft minimum guard requirements are in Chapter 5 of this Manual).

a. 4125 kilohertz (kHz) High Frequency (HF) Radiotelephony. GMDSS voice frequency that has a dual role as a distress and hailing voice frequency.

b. Very High Frequency (VHF) Radiotelephony.

(1) VHF-FM Channel 9 (156.45 MHz). The increasing volume of radio calls, primarily between recreational vessels, exceeds the capacity of VHF-FM Channel 16 (156.800 MHz). VHF-FM Channel 9 (156.45 MHz) may be used by recreational vessels for

general purpose calling. This frequency must be used whenever possible to relieve congestion on VHF-FM Channel 16 (156.800 MHz). Safety and distress broadcasts must continue to be announced on VHF-FM Channel 16 (156.800 MHz).

(2) VHF-FM Channel 16 (156.800 MHz). 156.800 MHz is designated as an international distress, safety, and calling frequency for radiotelephony for stations of the maritime mobile service.

(3) VHF-FM Channel 22A (157.100 MHz). Designated as a working frequency between CG stations and stations of the maritime community, 157.1 MHz is used after initial contact is established on VHF-FM Channel 16 (156.800 MHz).

(4) Very High Frequency – Amplitude Modulated (VHF-AM) 121.5 MHz and 123.1 MHz. The aeronautical emergency frequency 121.5 MHz, also known as International Air Distress (IAD), is a VHF frequency used for distress and urgency communications of the aeronautical mobile service. 123.1 MHz is the aeronautical auxiliary frequency used by stations of the aeronautical mobile service and by other mobile and land stations engaged in coordinated search and rescue operations. Passenger ships and ships operating in polar waters are required to have the means for two-way on-scene and SAR coordination voice communications with aircraft on 121.5 and 123.1 MHz.

c. Ultra High Frequency (UHF) 243.0 MHz. The aeronautical emergency frequency 243.0 MHz, also known as Military Air Distress (MAD), is designated as an international survival craft and U.S. military common emergency frequency used to provide rescue communication between aircraft, manned space vehicles, ground stations, or surface craft. Military aircraft and survival craft can use this frequency for EPIRBs and to broadcast urgent or safety messages.

d. Testing of equipment on 121.5 MHz and 243.0 MHz should be coordinated with appropriate authorities and completed in the first five minutes of each hour.

6. Distress Beacons. An Emergency Position-Indicating Radio Beacon (EPIRB) is a maritime alert devices used for distress alerting and locating survivors of distress incidents through 406 MHz distress beacons. The 406 MHz distress alerting signal is a short digital burst approximately every 50 seconds and the low power 121.5 MHz homing signal on the EPIRB is comprised of an upward-sweeping tone.

a. Aircraft on international flights are required to carry the 406 MHz distress beacon as their emergency locator transmitter (ELT), but national regulation can allow the use of the 121.5 MHz ELT on domestic routes. ELTs are built to survive the tremendous force of an aircraft crash. However, they are carried inside the aircraft and are usually less waterproof and non-floating. Aircraft ELTs must meet FAA regulations.

b. Personal locator beacons (PLB) are 406 MHz distress beacons used in the maritime community, as well as ashore, and can be automatically activated.

c. Cosmicheskaya Sistyema Poiska Avariynich Sudov - Search and Rescue Satellite-Aided Tracking (COSPAS – SARSAT) System. COSPAS-SARSAT is an international satellite based search and rescue system established by the U.S., Russia, Canada, and France to locate

406 MHz distress beacons (EPIRB/ELT/PLB). The COSPAS-SARSAT system does not detect the 121.5 MHz signal.

d. Emergency Position-Indicating Radio Beacon (EPIRB) Classes.

(1) Category I – 406/121.5 MHz Homing Signal. Free-floating, automatically activated, and detectable by satellites anywhere in the world. This type of EPIRB is recognized by GMDSS.

(2) Category II – 406/121.5 MHz Homing Signal. Similar to Category I, but manually activated. Some models are also water activated.

7. Terminating False Emergency Position-Indicating Radio Beacon (EPIRB) Signals. Under the provisions set forth in 14 U.S.C. § 521, the CG, in performing its maritime SAR mission, must perform any and all acts necessary to rescue and aid persons and protect and save property. The procedures for terminating EPIRB signals can be found in Reference (a).

8. Search and Rescue Transponder (SART). The radar SART, operating in the 9200-9500 MHz frequency band, is a transponder used for locating survival craft using an X-Band Radar.

a. The SART signal appears as a distinctive line of 12 equally spaced blips (dots) on the radar screen extending outward from the SART position along its line of bearing;

b. Unique signals (swept frequency) are generated for interpretation only after being triggered by 9 GHz ship or aircraft radar;

c. The detectable range from the air is approximately 40 nautical miles; surface is approximately 10 nautical miles;

d. An audible alarm or light is activated on the SART when a rescue ship or aircraft is within close range;

e. The battery capacity is rated for a minimum of 96 hours.

9. Automatic Identification System-Search and Rescue Transmitter (AIS-SART). This is a SAR transmitter used for locating survival craft. The AIS-SART may be used in lieu of the radar SART discussed above. It transmits messages from the survival craft received and displayed on AIS installations (SOLAS regulated ships are required to carry AIS installations). The position and time synchronization for the class A position report is derived from a built in Global Navigation Satellite System (GNSS) receiver (e.g., global positioning system (GPS)) and updated at a rate of once a minute. The AIS-SART operates on VHF-FM Channels 87B (161.975 MHz) and 88B (162.025 MHz).

a. The AIS-SART message indicates the position and safety information of the unit in distress.

b. The AIS-SARTs is detectable at a range of approximately five nautical miles over water.

c. The AIS-SART provides a continuous transmission even if the position and time synchronization from the positioning system is lost or fails.

d. The AIS-SART begins to transmit within 60 seconds of activation.

e. The battery capacity is rated for a minimum of 96 hours.

CHAPTER 12 COAST GUARD (CG) AUXILIARY

A. General. This Chapter provides policy specific to CG Auxiliary communications. Additional information, regarding Auxiliary communications and operations can be found in the Auxiliary Operations Policy Manual, COMDTINST M16798.3 (series).

B. Communications Command (COMMCOM). Commanding Officer, COMMCOM serves as the CG Program Manager for CG Auxiliary Communications.

C. CG Auxiliary Communication Network.

1. COMMCOM must be responsible for control of the CG Auxiliary communication network to include the provision of training and drills to CG Auxiliary personnel.
2. The Area Commander, District Commander, COMMCOM, or Commandant (CG-672) may designate frequencies specifically authorized for CG Auxiliary use.
3. Auxiliary use of designated frequencies must be limited to the duration of an incident or event such as contingency communications, COOP, regattas, coordinated training, or other official events requiring CG Auxiliary participation.

D. CG Auxiliary Interpreter Corps. The Interpreter Corps consists of over 440 volunteer Auxiliary members who possess a high proficiency in 48 foreign languages that can be used for interpretation during operational missions when persons in distress do not speak/understand English or when working with assisting foreign agencies or resources. The listing of CG Auxiliary Interpreter Corps volunteers and the languages spoken can be accessed at: http://icdept.cgaux.org/.

E. CG Auxiliary Communication Policy.

1. Keyed Very High Frequency-Frequency Modulated (VHF-FM) and Ultra High Frequency (UHF) Handheld Radios. CG Auxiliary personnel are authorized to use SBU keyed VHF-FM and UHF handheld radios to support CG operations.
2. CG Auxiliary Handheld Radio Issuance. Units are authorized to issue keyed handheld radios to CG Auxiliary personnel. The unit must ensure the following prior to issuing the keyed handheld radio:
   a. The CG Auxiliary member is qualified as CG Auxiliary communications operator per local unit requirements;
   b. The CG Auxiliary member has a signed Non-Disclosure Agreement, DHS Form 11000-6, on file;
   c. The CG Auxiliary member has a letter on file, signed by the CG orders issuing authority, authorizing use, possession and custody of keyed handheld radios; and,
   d. The CG Auxiliary member has completed unit training in keyed radio operations, storage, transportation, reporting loss/stolen keyed radios, and OTAR capabilities/operation.
3. CG Auxiliary Handheld Radio Use. CG Auxiliary personnel must:
   a. Operate the radio only while under CG orders;
   b. Operate keyed radios per approved Annex K to Area OPLAN, District Annex K or supplement, and local SOPs;
   c. Not maintain custody of physical cryptographic keymat or physical loading devices; and,

d. Not maintain personal custody of keyed radios unless specifically authorized to do so by higher authority.

4. Cryptographic Keying Material (Keymat) Loads.

   a. The loading of cryptographic keymat in radios distributed to CG Auxiliary personnel must be limited to authorized CG personnel at the CG unit to which assigned or at an authorized CG support unit; and,

   b. Authorization to load cryptographic keymat can be assigned to another CG unit on a limited case-by-case basis only.

5. Telephony Policy. Per Chapter 3 of this Manual, Auxiliary members are not authorized federal calling cards or the use of DSN services.

6. Broadcast Quality Control Monitoring Program. Area Commanders must engage the CG Auxiliary where appropriate to assist in CG broadcast quality control monitoring efforts. This engagement must be initiated and managed through the Auxiliary Department of Operations Communications Division at the national level (AUX-DVC-OT) who must designate an Auxiliary command POC for the COMMCOM.

F. CG Auxiliary Aircraft.

1. Restricted Use of VHF Channel 70 (156.525 MHz). CG Auxiliary aircraft must not use Channel 70 (156.525 MHz) for other than SAR related communications with maritime mobile stations in the maritime mobile service. See Chapter 5 for additional guidance specific to CG aircraft communications.

2. Maritime Mobile Service Identity (MMSI). The issuance of an MMSI to CG Auxiliary aircraft requires a written agreement between Commandant (CG-672) and authorized Auxiliary Air Facility specifying understanding that the DSC radio must only be used for SAR operations.

APPENDIX A - LIST OF ACRONYMS

Acronym	Definition
ACD	Automatic Call Distribution
ACP	Allied Communications Publication
ADCON	Administrative Control
ADMIN OIX	Administrative Official Information Exchange
AES	Advanced Encryption Standard
AIG	Address Indicator Group
AIS	Automatic Identification System
AIS-SART	Automatic Identification System Search and Rescue Transmitter
ALCGCIV	All Coast Guard Civilian
ALCGENL	All Coast Guard Enlisted
ALCGFINANCE	All Coast Guard Finance
ALCGOFF	All Coast Guard Officer
ALCGPSC	All Coast Guard Personnel Service Center
ALCGRECRUITING	All Coast Guard Recruiting
ALCGRSV	All Coast Guard Reserve
ALCOAST	All Coast Guard
ALE	Automatic link establishment
ALTERS	Allied Telecommunications Record System
ANI	Automated number identification
AOR	Area of responsibility
APEL	Allied Publication Electronic Library
ATC	Authority to connect
ATCA	Automatic test call answering

Acronym	Definition
ATO	Authority to Operate
ARQ	Automatic repeat request
BNM	Broadcast Notice to Mariners
BRI	Basic Rate Interface
C2OIX	Command and Control Official Information Exchange
C4	Command, control, communications, and computers
C4I	Command, control, communications, computers, and intelligence
C4ISR	Command, control, communications, computers, intelligence, surveillance and reconnaissance
C4IT	Command, control, communications, computers, and information technology
C5ISC	Command, Control, Communications, Computers, Cyber and Intelligence Service Center
CA	Command Authority
CAD	Collective address designator
CALLER ID	Caller Identification
CART	Command assessment of readiness and training
CAS	Collaboration at sea
CASREP	Casualty report
CAT	Communications assist team
CB	Citizens Band
CBP	Customs and Border Protection
CC	Command Center
CCI	Cryptographically Controlled Item

Acronym	Definition
CCP	Contingency Communications Plan
CDR	Call Detail Recording
CEP	Continuous Evaluation Program
CFR	Code of Federal Regulations
CG	Coast Guard
CGCS	Coast Guard Communication System
CGCYBER	Coast Guard Cyber Command
CGES	Coast Guard Exchange System
CGOne	Coast Guard One Network
CIC	Combat information center
CIO	Chief Information Officer
CJCS	Chairman, Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CMCS	COMSEC Material Control System
CMDAUTH	Command Authority
CMS	COMSEC Material System
CNO	Chief of Naval Operations
COLNAV	Columbian Navy
COMCGCYBER	Commander, Coast Guard Cyber Command
COMDTINST	Commandant Instruction
COML	Communications Unit Leader
COMMCOM	Communications Command
COMMDET	Communications Detachment
COMMSHIFT	Communication guard shift
COMMSYS	Communication System

Acronym	Definition
COMNAVSECGRU	Commander, Naval Security Group Command
COMSATCOM	Commercial satellite communication
COMSEC	Communications security
COMSPOT	Communication spot
COMTAC	Communications tactical
CONAUTH	Controlling Authority
COP	Common Operational Picture
COOP	Continuity of operations
COR	Central Office of Record
COS	Class of service
COSPAS-SARSAT	Cosmicheskaya Sistyema Poiska Avariynich Sudov – Search and Rescue Satellite-Aided Tracking
COTHEN	Cellular over the Horizon Enforcement Network
CRF	Crypto Repair Facility
CSO	Command Security Officer
CSOC	Cyber Security Operations Center
CSN	Communication Systems Network
CUAS	Common User Application Software
CUDIXS	Common User Digital Information Exchange System
DAMA	Demand assigned multiple access
DAR	Designated agency representatives
DCMS	Deputy Commandant for Mission Support
DCO	Deputy Commandant for Mission Operations
DCS	Defense Communications System

Acronym	Definition
DES	Data encryption standard
DF	Direction finding
DHS	Department of Homeland Security
DHS OneNet	Department of Homeland Security One Network
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DMD-PS	Data Management Device – Power Station
DNI	Director of National Intelligence
DOD	Department of Defense
DODIN	Department of Defense Information Network
DRS	Disaster Recovery System
DSC	Digital selective calling
DSL	Digital subscriber line
DSN	Defense System Network
DTG	Date-time group
DVL	Digital voice logger
EA	Enterprise Architecture
EAIS	Encrypted Automatic Identification System
EGC	Enhanced group call
EHF	Extremely high frequency
EMSS	Enhanced Mobile Satellite Service
ELMR	Enterprise land mobile radio
ELT	Emergency locator transmitter
Email	Electronic mail
EMCOM	Emission control

Acronym	Definition
EMICP	Enhanced Mobile Incident Command Post
EMSEC	Emission security
EO	Executive Order
EPIRB	Emergency position-indicating radio beacon
ESD	Electronic Systems Support Detachment
ESU	Electronic Systems Support Unit
FAA	Federal Aviation Administration
FAX	Facsimile
FCC	Federal Communications Commission
FEC	Forward error correction
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FORCECOM	Commander Forces Readiness Command
FOUO	For official use only
FRC	Federal Records Center
FRS	Family Radio Services
FSD	Field Services Division
FSS	Fixed Satellite Service
FTS	Federal Telephone Service
FXP	Fleet Exercise Publication
GENADMIN	General administrative
GETS	Government Emergency Telecommunications Service
GMDSS	Global Maritime Distress and Safety System

Acronym	Definition
GMF	General Message File
GMRS	General Mobile Radio Services
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSA	General Services Administration
GSCR	Generic Switching Center Requirements
GSM	Global security module
HF	High frequency
HF-ALE	High frequency-automatic link establishment
HIPAA	Health Insurance Portability and Accountability Act
HLS Net	Homeland Security Network
HSPD	Homeland Security Presidential Directive
IA	Information assurance
iApp	Intermediary Application (iApp)
IAMSAR	International Aeronautical and Maritime Search and Rescue Manual
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IMEI	International Mobile Equipment Identity
IMH	Incident Management Handbook
IMO	International Maritime Organization
IMPAC	International merchant purchase authorization card
INFOSEC	Information security
INTERCO	International Code of Signals
IOP	Interoperability

Acronym	Definition
IP	Internet Protocol
IRR	International Radio Regulations
ISDN	Integrated Services Digital Network
ISIC	Immediate-superior-in-command
ISM	Iridium security module
ISSO	Information Systems Security Officer
ITOC	IT Operations Center
ITU	International Telecommunications Union
IW	Integrated Wave Form
IWN	Integrated Wireless Network
JANAP	Joint Army, Navy, Air Force Publication
JIACC	Joint Inter-agency Counterdrug COMSEC
JIATF	Joint Interagency Task Force
JIST	Joint Integrated Satellite Communications Tool
JITC	Joint Interoperability Test Command
JSIR	Joint Spectrum Interference Report
JWICS	Joint Worldwide Intelligence Communications Systems
kbps	Kilobits per second
Keymat	Keying material
kHz	Kilohertz
KMF	Key Management Facility
KMI	Key Management Infrastructure
KVL	Key variable loader
LANTAREA	Atlantic Area

Acronym	Definition
LCMS	Local COMSEC Management Software
LE	Local Element
LE(I)	Local Element (Issuing)
LEC	Local exchange carrier
LE Sensitive	Law enforcement sensitive
LOA	Letter of Agreement
MARS	Military Auxiliary Radio System
MCC	Mobile contingency communications
MCV	Mobile communication vehicle
MEDICO	Medical communications
MF	Medium frequency
MGC	Management Given Client
MHz	Megahertz
MILSATCOM	Military satellite communication
MISLE	Marine Information for Safety and Law Enforcement
MMR	Mobile Maritime Radio
MMSI	Maritime mobile service identity
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multi-protocol label switching
MRASS	Mariner Radio Activated Sound Signal device
MSS	Mobile Satellite Service
MUOS	Mobile User Objective System
MURS	Multi User Radio Service
NAFI	Non-Appropriated Funds Instrumentalities

Acronym	Definition
NAIS	Nationwide Automatic Identification System
NATO	North Atlantic Treaty Organization
NAVAREA	Navigational area
NAVCEN	Coast Guard Navigation Center
NAVIFOR	Navy Information Forces
NAVPUB	Naval Publication
NAVTEX	Navigational Telex
NCA	National Command Authority
NCMS	Naval Communication Security Material System
NCS	National Communications System
NCTAMS	Naval Computer and Telecommunications Area Master Station
NDLS	Navy Doctrine Library System
NDP	Naval Doctrine Publication
NDRS	National Distress and Response System
NECN	National Emergency Communications Network
NECOS	Net control station
NGA	National Geospatial-Intelligence Agency
NIFOG	National Interoperability Field Operations Guide
NIMS	National Incident Management System
NIPRNET	Non-classified internet protocol router network
NIST	National Institute of Standards and Technology
NLECC	National Law Enforcement Communications Center
NOAA	National Oceanic and Atmospheric Administration
NORTHCOM	U.S. Northern Command

Acronym	Definition
NSA	National Security Agency
NS/EP	National security and emergency preparedness
NSI	National security information
NSS	National Search and Rescue Supplement
NSPD	National Security Systems Policy Directive
NTIA	National Telecommunications and Information Administration
NTISSD	National Telecommunications and Information Systems Security Directive
NTP	Naval Telecommunications Procedures
NTRP	Navy Tactical Reference Publications
NTTP	Naval Tactics, Techniques, and Procedures
NWDC	Navy Warfare Development Center
NWEL	Navy Warfare Electronic Library
NWL	Naval Warfare Library
NWP	Naval Warfare Publications
NWS	National Weather Service
OEC	Office of Emergency Communications
OFCO	Operating Facility Change Order
OMB	Office of Management and Budget
OPCON	Operational control
OPLAN	Operations plan
OPNAVINST	Office of the Chief of Naval Operations Instructions
OPORDER	Operational order
OPSEC	Operations security
OPTASK	Operational tasking

Acronym	Definition
ORD	Operational Requirements Document
OS	Operations specialist
OSHA	Occupational Safety and Health Act
OTAR	Over the air rekeying
P25	Project 25
PACAREA	Pacific Area
PBX	Private branch exchange
PCII	Protected critical infrastructure information
PERSEC	Personnel security
PII	Personal identifiable information
PIN	Personal identification number
PLAD	Plain language address designator
PLB	Personal Locator Beacon
PLT1RA	Personnel Local Type 1 Registration Authority
PRL	Publication Requirement List
PROFORMA	Pre-formatted
PSTN	Public Switched Telephone Network
RESCUE 21	Rescue 21
RADIOFAX	Radio facsimile
RADLOGS	Radio logs
RCC	Rescue coordination center
RCF	Remote communications facility
RFCOMM-CTM	Radio Frequency Communications – Core Technology Manager
RFF	Remote fixed facility

Acronym	Definition
RPC	Regional Planning Committee
RP	Resource proposal
RPWIN	Remote Programming Window
RSKL	Really Simple Key Loader
SAR	Search and Rescue
SART	Search and Rescue Transponder
SASS	Sea, Air, Shore Secure
SATHICOM	Satellite high command
SBU	Sensitive but unclassified
SCC	Sector Command Center
SCI	Sensitive compartmented information
SECDEF	Secretary of Defense
SECDHS	Secretary, Department of Homeland Security
SECNAV	Secretary of Navy
SERVAUTH	Service Authority
SHARES	Shared resources
SHD	Special handling designator
SIM	Subscriber identity module
SIPRnet	Secret internet protocol router network
SITOR	Simplex teletype over radio
SKL	Simple Key Loader
SMC	SAR mission coordinator
SMIB	Safety Marine Information Broadcast
SOLAS	Safety of life at sea
SOP	Standard operating procedure

Acronym	Definition
SOSO	Speed of service objective
SOW	Statement of Work
SPII	Sensitive personal identifiable information
STE	Secure telephone equipment
TACCOM	Tactical communication
TACON	Tactical control
TASK	Task organization
TCO	Telecommunications Certification Office
TCTO	Time compliance technical order
TRANSEC	Transmission security
TS	Top Secret
TSO	Token Security Officer
TSTA	Tailored ships training availability
TTP	Tactics, techniques and procedures
UC	Unified communications
UHF	Ultra-high frequency
UHF-AM	Ultra-high frequency – amplitude modulated
UMIB	Urgent marine information broadcast
UNCLOG	U.S. Coast Guard / National Weather Service Coordination-Liaison Working Group
UPS	Uninterruptible power supply
U.S.C.	U.S. Code
USN	U.S. Navy
UTC	Coordinated universal time

Acronym	Definition
VDL	Virtual data link
VDLS	Vaults, Depot, and Logistics System
VHF	Very high frequency
VHF-FM	Very high frequency – frequency modulated
VM	Voice mail
VOBRA	Voice broadcast automation
VoIP	Voice over internet protocol
VTC	Video teleconferencing
VTS	Vessel Traffic Service
WAN	Wide area network
WPS	Wireless priority service

APPENDIX B GLOSSARY

Term	Definition
Abbreviated Log	An electronic or handwritten communication log that contains a synopsis of all tactical and maritime public safety communication data a unit transmits or receives. Verbatim entries are not required.
Address Indicating Group (AIG)	An address designator used in record messaging that represents a list of specific and frequently recurring combination of action and/or information addressees
Administrative Official Information Exchange (Admin OIX)	Renamed to command Email. Communications means using command shared mailboxes for the exchange of official administrative information.
Code Plug	A program loaded into the radio that provides dedicated frequencies used to transmit and receive, radio frequency power output, carrier squelch/coded squelch, signaling modes, and other special features that need to be enabled.
Commercial Satellite Communications (COMSATCOM)	Includes any satellite communication equipment or capabilities which can be acquired from the public sector.
Communications Guard	The Glossary of Communications Electronic Terms, ACP 167 (series), defines guard (radio communication) as “to maintain a continuous receiver watch with transmitter ready for immediate use.”
Communication Log	An official record of signals transmitted and received by a radio equipped unit.
Complete Log	A manually completed (i.e., paper, electronic) or recorded (i.e. RESCUE 21 system, DVL) communication log that contains all tactical and marine public safety communication data a unit transmits or receives.

Term	Definition
Command and Control (C2)	The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.
Communication Security (COMSEC) Material	Item designed to secure or authenticate communications. COMSEC material includes, but is not limited to cryptographic keying material (KEYMAT), equipment, devices, documents, call signs and authenticators, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.
Communications Security (COMSEC) Material Control System (CMCS)	Logistics and accounting system used to distribute, control, and safeguard COMSEC material marked "CRYPTO." CMCS includes the COMSEC Central Offices of Record, crypto logistic depots, and COMSEC accounts. COMSEC material other than cryptographic keying material (KEYMAT) can be handled through the CMCS (See KMI definition).
Communication Security (COMSEC) monitoring	The act of listening to, copying, or recording transmissions of one's own official communication to analyze the degree of security.
Continuous Guard	The operator must monitor the required frequency unless required to transmit on another frequency. After transmission, the operator must immediately switch back to the guarded frequency.
Daily Communications Log	Official records, documenting communication and related events concerning the command. Communication logs also provide a record that can be the subject of investigation or legal action.
Decryption	The process of converting encrypted data (cipher text) back into its original form.

Term	Definition
Demand Assigned Multiple Access (DAMA)	DAMA multiplexes several baseband systems or users onto one 25 kilohertz (kHz) channel to increase the number of available channels. One 5 kHz DAMA channel can support one 2.4 kilobits-per second (kbps) voice time slot and one point-to-point connection. One 25 kHz DAMA channel can support up to five 2.4 kbps voice or data circuits.
Coast Guard Boat	Vessels less than 65' in length.
Coast Guard Cutter	Vessels 65' and greater in length.
Collective Address Designator (CAD)	A single group that represents a predetermined set of activities linked by an operational or administrative chain-of command.
Command and Control Official Information Exchange (C2OIX)	Record message communication system used for the exchange of operational information only.
Emission Control (EMCON)	EMCON is the procedure used to provide transmission security (TRANSEC) through control of all electromagnetic and acoustic radiations, including communication, radar, electronic warfare, and sonar. In addition, EMCON can be an effective tool for implementing low probability of intercept (LPI), low probability of detection (LPD), and low probability of identification (LPID).
Emission Security (EMSEC)	Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emanations from crypto-equipment or an information system. (See TEMPEST definition).
Encryption	The process of changing plaintext into cipher text than cannot be understood by unauthorized entities for the purpose of security or privacy.
Enhanced Mobile Satellite Service (EMSS)	Designates the "enhanced" form of Iridium mobile satellite communications and includes a secure capability, the ability to direct dial from a Public Switched Telephone Network phone to the 808 area code, and the ability to communicate with the DSN.
Fixed Satellite Service (FSS)	COMSATCOM equipment that can be used to communicate only while the transmit/receive equipment is stationary.

Term	Definition
Information Assurance (IA)	The practice of assuring information and managing risks related to the use, processing, storage, and transmission of information and the systems and processes used for those purposes.
Information Security (INFOSEC)	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
Integrated Waveform (IW)	IW is a recently implemented UHF satellite communication (SATCOM) waveform which requires software and/or hardware upgrades to existing UHF SATCOM terminals. Using legacy DAMA, this waveform increases the UHF SATCOM channel availability allowing SATCOM planners the ability to mitigate any potential Mobile User Objective System (MUOS) schedule delays or UHF SATCOM constellation failures.
Interim Polar System	The Interim Polar System provides users only low data-rate EHF access and does not have the ability to cross-link to the UHF Follow-on (UFO) constellation. There is limited infrastructure in place for Interim Polar System communications support.
Joint Tactical Radio System (JTRS)	JTRS is a new generation multi-band radio system, developed by the DOD, to replace existing MILSATCOM terminals. JTRS radios are compatible with the MUOS satellites and provide a variety of waveforms, including MUOS, to access the on-demand 2.4 to 64 kbps channels for voice and data services.
Key Management Infrastructure (KMI)	KMI is the program that COMSEC keying material is; accessed, accounted for, delivered, and ordered.
Legacy Military Satellite Communications (MILSATCOM)	Legacy MILSATCOM refers to all MILSATCOM equipment not IW capable (e.g., LST-5D, TD-1271).
Maritime Mobile Service Identity (MMSI) Number	A nine-digit number used by maritime DSC, AIS, and certain other equipment to uniquely identify a ship or a coast radio station.

Term	Definition
Military Satellite Communications	MILSATCOM is the DOD satellite constellation providing near global operational communications for military aircraft, ships, and ground stations to meet the requirements for rapid, reliable, and secure communications throughout DOD. The CG requires access to MILSATCOM for interoperability with the USN and DOD in time of war (14 U.S.C. § 103(b)), to meet CG, DHS, and interagency missions in peacetime and for communicating with U.S. allies and other government agencies.
MINIMIZE	A term, not acronym, used by command authorities to clear military communication circuits of all nonessential traffic in an actual, simulated, or anticipated emergency. This includes, but is not limited to, record messaging systems, Email (to include attachment size limitations), CGOne, SIPRnet, JWICS, telephone and cellular circuits, chat, internet, social media, and video teleconferencing use.
Mobile Satellite Service (MSS)	COMSATCOM equipment that can be used to communicate while the device is in motion. CG cutters are equipped with MSS equipment provided via multiple vendors.
Mobile User Objective System (MUOS)	A limited protected narrowband (64 kbps and below) satellite communication system that supports a worldwide, multiservice population of mobile and fixed site terminal users.
Multi-band Radio	A radio that can operate in more than one frequency band.
Non-Demand Access Multiple Access (DAMA)	Non-DAMA refers to the use of a single 5 kHz or 25 kHz channel for MILSATCOM circuits when a DAMA channel would not be suitable.
Operations Security (OPSEC)	OPSEC is an analytical process used to deny an adversary information- generally unclassified – concerning CG intentions and capabilities by identifying, controlling, and protecting indicators associated with CG planning processes or operations.
Originator	Person, organization, or unit responsible for the initiation of a message. Units rebroadcasting messages provided via other means (e.g., NOAA weather) are not considered the originator.
Plain Language Address (PLA)	Unit identifier used in record messaging.

Term	Definition
Protected Communication	Communications using unclassified or "Type III" encryption including data encryption standard (DES) or advanced encryption standard (AES) encryption.
Radio Logs (RADLOGS)	A software logging program used at the COMMCOM. AIRSTA Kodiak has a single component of RADLOGS called Electronic Status Board.
River City	Nested Security Groups - roles based Access Control – for underway units to protect their mission resource requirements by limiting access to operational People & Computers as need to protect their mission resource requirements by limiting access to operational People & Computers as needed.
Safety Marine Information Broadcast (SMIB)	Contain important navigational and meteorological warnings, sunspot activity, or other unusual events that might impact maritime activities.
Scheduled Broadcast Notice to Mariners	Include search and rescue, navigational, hydrographic, or weather information.
Secure Communication	Communication using classified or "Type I" encryption to support classified information exchange.
Tactical Communications	Near-real time or real time communication supporting an ongoing CG operation.
Telecommunication	Communication over a distance (as by cable, telegraph, telephone, or broadcasting).
TEMPEST	An unclassified cover term (not an acronym) used to identify anything relating to the study of unintentional compromising emanations.
Transmission Security (TRANSEC)	Security controls applied to transmissions to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals. TRANSEC is that field of COMSEC which deals with the security of communication transmissions, rather than that of the information being communicated (see EMCON definition).

Term	Definition
Unauthorized Disclosure	Any classified, SBU, PII item listed in the CG Critical Information List (CIL), Essential Elements of Friendly Information (EEFI) list or material that has been transmitted via an unauthorized method and results in a possible exposure of this information or material to unauthorized individuals.
Uninterrupted Guard	The operator can switch to another frequency to make a transmission, but must maintain monitoring the frequency that requires the uninterrupted guard.
Urgent Marine Information Broadcast (UMIB)	Concern the safety of a ship, aircraft, other vehicle, or the safety of a person.

APPENDIX C PUBLIC MARITIME BROADCASTS SCHEDULES

1. VHF-FM Broadcast Schedule. Exhibit C-1 lists the VHF-FM time of scheduled broadcasts by District for each transmission facility listed.
2. HF Voice Broadcast Schedule. Exhibit C-2 is the HF VOBRA broadcast schedule for CG transmission facilities listed.
3. HF SITOR Broadcast Schedule. Exhibit C-3 is the HF SITOR broadcast schedule for CG transmission facilities listed.

Exhibit C-1 - Sector VHF-FM Time of Scheduled Broadcasts

First Coast Guard District **VHF Voice and Weather Broadcast CH 16/22**	
Sector Northern New England	1105Z, 2305Z
Sector Boston	1035Z, 2235Z
Sector Southeastern New England	1005Z, 2205Z
Sector Long Island Sound	1120Z, 2320Z

Fifth Coast Guard District **VHF Voice and Weather Broadcast CH 16/22**	
Sector Delaware Bay	1103Z, 2303Z (Coastal) 1235Z, 0035Z (Rivers)
Sector Maryland National Capital Region	0130Z, 1205Z
Sector Virginia	0230Z, 1120Z
Sector North Carolina	Warnings only - 0130Z North, 0155Z South, 1030Z South, 1055Z North

Seventh Coast Guard District VHF Voice and Weather Broadcast CH 16/22	
Sector Charleston	1200Z, 2200Z
Sector Jacksonville	Warnings only
Sector Miami	Warnings only
Sector Key West	1200Z, 2200Z
Sector San Juan	1210Z, 2210Z
Sector St. Petersburg	1300Z, 2300Z

Eighth Coast Guard District VHF Voice and Weather Broadcast CH 16/22	
Sector Ohio River Valley	None
Sector Upper Mississippi River	None
Sector Lower Mississippi River	None
Sector Mobile	1020Z, 1220Z, 1620Z, 2220Z
Sector New Orleans	1035Z, 1235Z, 1635Z, 2235Z
Sector Houston-Galveston	1050Z, 1250Z, 1650Z, 2250Z
Sector Corpus Christi	1040Z, 1240Z, 1640Z, 2240Z

Ninth Coast Guard District **VHF Voice and Weather Broadcast CH 16/22**	
Sector Buffalo	0255Z, 1455Z
Sector Detroit	0135Z, 1335Z
Sector Lake Michigan	0255Z, 1455Z
Sector Sault Ste. Marie	0005Z, 1205Z

Eleventh Coast Guard District VHF Voice and Weather Broadcast CH 16/22	
Sector Humboldt Bay	1615Z, 2315Z
Sector San Francisco	1630Z, 1900Z, 2130Z(winter)
Sector Los Angeles/Long Beach	0200Z, 1800Z
Sector San Diego	0100z, 1700z

Thirteenth Coast Guard District VHF Voice and Weather Broadcast CH 16/22	
Sector Pugent Sound	0630Z, 1830Z
Sector Columbia River	1745Z
Sector North Bend	0603Z, 1803Z

Fourteenth Coast Guard District VHF Voice and Weather Broadcast CH 16/22	
Sector Honolulu	0500Z, 1700Z
Sector Guam	0900Z, 2100Z

Seventeenth Coast Guard District VHF Voice and Weather Broadcast CH 16/22	
Sector Juneau	None
Sector Anchorage	None

Note: The USCG has elected not to broadcast forecasts or warnings from Sectors Juneau and Anchorage as coverage overlaps with NOAA Weather Radio.

Exhibit C-2 - HF Voice Broadcast Schedule

COMMCOM Chesapeake (NMN) **HF Voice Broadcast Schedule**						
4426, 6501, 8764 kHz (USB)	0330Z[1]	0515Z[2]	0930Z[1]			
6501, 8764, 13089 kHz (USB)			1115Z[2]	1530Z[1]	2130Z[1]	2315Z[2]
8764, 13089, 17314 kHz (USB)				1715Z[2]		
[1] Offshore Forecasts, hurricane information [2] Highseas Forecast, hurricane information Broadcast of hurricane and other weather broadcasts from this station may on occasion be preempted, as the frequencies are shared with other USCG stations.						

COMMCOM RCF New Orleans (NMG) **HF Voice Broadcast Schedule**								
4316, 8502, 12788 kHz (USB)	0330Z[1]	0515Z[2]	0930Z[1]	1115Z[2]	1530Z[1]	1715Z[2]	2130Z[1]	2315Z[2]
[1] Offshore Forecasts, hurricane information [2] Highseas Forecast, hurricane information Broadcast of hurricane and other weather broadcasts from this station may on occasion be preempted, as the transmitters are shared with the radiofax broadcast.								

COMMCOM RCF Pt. Reyes (NMC) **HF Voice Broadcast Schedule**				
4426, 8764, 13089 kHz (USB)	0430 Z	1030 Z		
8764, 13089, 17314 kHz (USB)			1630Z	2230Z
Broadcast of hurricane and other weather broadcasts from this station may on occasion be preempted, as the frequencies are shared with other USCG stations, and the transmitters are shared with the radiofax broadcast.				

COMMDET Kodiak (NOJ) **HF Voice Broadcast Schedule**			
6501 kHz (USB)	0203Z		1645Z

COMMCOM RCF Honolulu (NMO) **HF Voice Broadcast Schedule**				
6501, 8764 kHz (USB)		0600 Z	1200 Z	
8764, 13089 kHz (USB)	0005Z			1800Z

Sector Guam (NRV) **HF Voice Broadcast Schedule**				
6501 kHz (USB)		0930 Z	1530 Z	
13089 kHz (USB)	0330Z			2130Z

Exhibit C-3 - HF SITOR Broadcast Schedule

RCF Boston (NMF) **HF SITOR (NBDP) Broadcast Schedule**		
6314, 8416.5, 12579 kHz	0140Z[3]	
8416.5, 12579, 16806.5 kHz		1630Z
[3]Includes International Ice Patrol		

RCF Pt. Reyes (NMC) **HF SITOR (NBDP) Broadcast Schedule**		
8416.5, 16806.5 kHz	0015Z	1730Z

RCF Honolulu (NMO) HF SITOR (NBDP) Broadcast Schedule				
8416.5, 12579, 22376 kHz	0130Z			2030Z
8416.5, 12579 kHz		0730Z	1330Z	

Sector Guam (NRV) **HF SITOR (NBDP) Broadcast Schedule**						
	0230Z[1]	0500Z	0900Z[1]	1500Z	1900Z	2315Z
[1]HYDROPAC navigation message, no weather						

Assigned frequencies shown, for carrier frequencies subtract 1.7 kHz. Typically specialized marine communications equipment uses assigned SITOR frequencies while general purpose equipment uses carrier frequencies. Note that stations share common frequencies.