U.S. Department of
Homeland Security

United States
Coast Guard

TELECOMMUNICATION MANUAL

COMDTINST M2000.3E
February 2012

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

Commandant
United States Coast Guard

2100 2nd St, S.W. Stop 7101
Washington, DC 20593-7101
Staff Symbol: CG-652
Phone: (202) 475-3535
Fax: (202) 475-3927

COMDTINST M2000.3E

FEB 07, 2012

COMMANDANT INSTRUCTION M2000.3E

Subj: TELECOMMUNICATION MANUAL

1. PURPOSE. This Manual establishes policy for the administration, management, and operation of the Coast Guard Telecommunication System.

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

3. DIRECTIVES AFFECTED. The Telecommunication Manual, COMDTINST M2000.3D is cancelled.

4. MAJOR CHANGES. Major changes to this Manual include:

   a. Updated to provide appropriate organizational alignment as a function of Modernization.

   b. Restructured and reorganized to improve the flow of information and eliminate repetition and duplication, including:

      (1) Consolidation of the previous Chapter 8 (Telecommunication and Network Services) into Chapter 5 (Special Communication Services).

      (2) Consolidation of Chapter 13 (Communication Area Master Stations (CAMS) and Communication Stations (COMMSTA) into Chapter 7 (Coast Guard Telecommunication Facilities and Functions).

      (3) Movement of detailed information on Electronic Key Management System (EKMS), Coast Guard Record Message System (CGRMS), and Rescue 21 System Configuration to Appendices (Appendix A, B and C).

DISTRIBUTION – SDL No. 159

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

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

c. Chapter 1 (old Chapter 3): Most affected by modernization updates.

d. Chapter 2 (old Chapter 1):

(1) Added telecommunications governance to provide authority for Coast Guard telecommunications.

(2) Telecommunication policy dissemination via messages added.

e. Chapter 3: Added requirements documents to provide additional explanation on the telecommunication requirements process.

f. Chapter 4: Type 1 and Type 2 encryption definitions removed since definitions for classified and sensitive/protected communications are now applied by the National Security Agency (NSA) and National Institute of Standards and Technology (NIST).

g. Chapter 5:

(1) Updated names of Coast Guard networks.

(2) Added internet policy as per U.S. Coast Guard Information Assurance (IA) for Unclassified Information Systems, COMDTINST 5500.13 (series).

(3) Added military satellite communication (MILSATCOM) section for MILSATCOM equipment acquisition and policy.

(4) Removed Coast Guard Auxiliary federal calling card procedures (Chapter 5).

h. Chapter 6:

(1) Updated search and rescue (SAR) records section as per current 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).

(2) Updated Retention of Files, Reports, Records, and Logs section per Information and Life Cycle Management Manual, COMDTINST M5212.12 (series).

(3) Added Audio File retention policy.

i. Chapter 7:

(1) Updated the list of services provided by CAMS/COMMSTA Kodiak.

(2) Updated reporting requirements for CAMS digital selective calling (DSC) Distress and Safety Statistics.

(3) Incorporated Small Boat communications section.

j. Chapter 9: Added Geo-Spatial over the Horizon ALE Matrix (GOTHAM) to aircraft communications.

k. Chapter 10:

(1) Included Electronic Mail (E-Mail), Chat Services and Text policy.

(2) Changed General Record Message retention period from 90 days to 1 year.

l. Chapter 12: Updated VHF-FM DSC Response policies for CG Afloat Units per 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).

m. Incorporated applicable policy elements of Commandant (CG-65) numbered Telecommunication Policy messages:

002/10: Maritime Channel Usage (Chapter 3)
004/10: Use of 800 MHz Channels (Chapter 3)
006/10: Standard CG VHF/UHF Standard Code Plugs (Chapter 3)
008/10: Iridium (Chapter 5)
009/10: National Weather Service Products for Broadcast (Chapter 13)
012/10: RESCUE 21 Direction Finding of Digital Selective Calling Distress Calls (Chapter 11)
013/10: Telephony Private Branch Exchange (PBX) Guidance (Chapter 5)
014/10: 2182 kHz Vessel Guard Requirements (Chapter 8)
015/10: Transition to Advanced Encryption (AES) (Chapter 4)
017/10: Bridge to Bridge Radio Telephone Act Policy (Chapter 8)
018/10: Updated Guidance on CG Participation in Federal/State/Local Wireless Voice Networks (Chapter 5)
002/11: Digital Selective Calling (Chapter 12)
003/11: Coast Guard Auxiliary Use of Keyed VHF-FM and UHF-FM Handheld Radios (Chapter 7)
005/11: Multi-Band Type-1 Tactical Radio Acquisition Policy (Chapter 5)
006/11: Standard Aviation Wulfsburg RT-5000 VHF/UHF Code Plugs and RPWIN Files (Chapter 9)
007/11: 2182 kHz Medium Frequency (MF) Sector Communications Guard Requirements (Chapter 11)
009/11: VHF/UHF CG-Wide Tactical Radio Frequency Plans and Supporting Code Plugs (Chapter 3)

n. Included an Index to facilitate location and correlation of information throughout the document.

5. REQUEST FOR CHANGES. Units and individuals may recommend changes by writing via the chain of command to: Commandant (CG-652); U. S. Coast Guard; 2100 2ND ST SW STOP 7101; Washington, DC 20593-0001.

6. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide operational guidance for Coast Guard personnel and is not intended to nor does it impose legally-binding requirements on any party outside the Coast Guard.

7. RECORDS MANAGEMENT CONSIDERATIONS. This Manual was thoroughly reviewed during the directives clearance process, and it has been determined there are records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., NARA requirements, and Information and Life Cycle Management Manual, COMDTINST M5212.12 (series).

8. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. The potential environmental impacts of this action have been carefully considered and found to be covered by Categorical Exclusion 1e (Figure 201, COMDTINST 16475.1(series)) as it is a guidance document that implements, without substantive change, the applicable Commandant Instruction, procedures, manuals and other guidance documents. None of the limitations noted in Chapter 2.B(2)(b)(2) of COMDTINST 16475.1 exist.

9. FORMS/REPORTS. The forms referenced in this Manual are available in USCG Electronic Forms on the Standard Workstation or on the Internet: http://www.uscg.mil/forms/; CG Portal https://cgportal.uscg.mil/delivery/Satellite/CG611/FORMS and Intranet at http://cgweb.comdt.uscg.mil/CGForms.

R. E. Day /s/
Assistant Commandant for Command, Control, Communications, Computers and Information Technology

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

TABLE OF CONTENTS

CHAPTER 1 COAST GUARD (CG) TELECOMMUNICATIONS ORGANIZATION

A. General. The Coast Guard Telecommunication System (CGTS) and its supporting organizations have undergone considerable change since the last production of this Manual. However, the purpose of the CGTS remains fundamentally unchanged. As specified in Department of Homeland Security (DHS) Management Directive 4800, "All organizational elements and agencies in DHS will function under the same policies, regulations, standards and rules pertaining to telecommunications operations." The CGTS is an essential resource under DHS, providing the means to share mission critical information with the Department of Defense (DOD) and federal, state, and local law enforcement officials to meet the objectives of defending our nation.

B. Coast Guard Telecommunication System (CGTS).

1. Definition. The CGTS is a telecommunication system of systems that links Coast Guard (CG) facilities (i.e., shore units, aircraft, cutters, boats) to other agencies and organizations throughout the nation and world. The CGTS refers to the radio, satellite, telephone, and network facilities that are 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 CGTS is to:

   a. Provide and maintain rapid, reliable, secure, and interoperable telecommunications to meet the operational requirements of CG forces along with other DHS components that use the Command, Control, Communication, Computers and Information Technology (C4&IT) infrastructure.

   b. Provide guidance on operational security as required by the National Communications System (NCS).

   c. Ensure connectivity, compatibility, and interoperability with National Command Authorities (NCA).

   d. Support the Global Maritime Distress and Safety System (GMDSS). GMDSS provides a means for the rapid and coordinated aid to vessels, persons, and aircraft in distress. The GMDSS also provides for urgency and safety communications and the transmission of maritime safety information (MSI), navigational and meteorological warnings and forecasts, and other urgent safety information to ships. GMDSS equipment requirements are mandatory for vessels subject to the Safety of Life at Sea (SOLAS) Convention of 1974. All cargo vessels 300 gross registered tons (GRT) and up, and all passenger ships engaged in international voyages, must be equipped with GMDSS systems that meet the international standards.

C. Coast Guard Telecommunication System (CGTS) Program Management Roles and Responsibilities. Program management of CGTS is a headquarters responsibility. It involves the planning, programming, and budgeting for CGTS along with national and international representation of CG interest.

1. Operational Communications Requirements Management. The CG's requirements management process is overseen by the Assistant Commandant for Capability (CG-7) and is outlined in Pub 7-7, Requirements Generation and Management Process.

2. Operational Communications Technical Authority. The operational communications technical authority is within the office of the Assistant Commandant for C4&IT (CG-6).

3. Communications Asset Management. Management oversight of currently deployed systems is the responsibility of the Assistant Commandant for C4&IT (CG-64).

4. Spectrum Management. Spectrum management is the responsibility of the Assistant Commandant for C4&IT (CG-65).

5. Information Assurance (IA) and Communication Security (COMSEC). IA and COMSEC are the responsibility of the Assistant Commandant for C4&IT (CG-65).

6. Communications Policy Management. Communications Policy Management and publication is within the office of the Assistant Commandant for C4&IT (CG-65).

7. Communications Doctrine, Tactics, Techniques and Procedures (TTP). The area telecommunication staffs are responsible for the development and dissemination of communications doctrine and TTP to include operational communications planning.

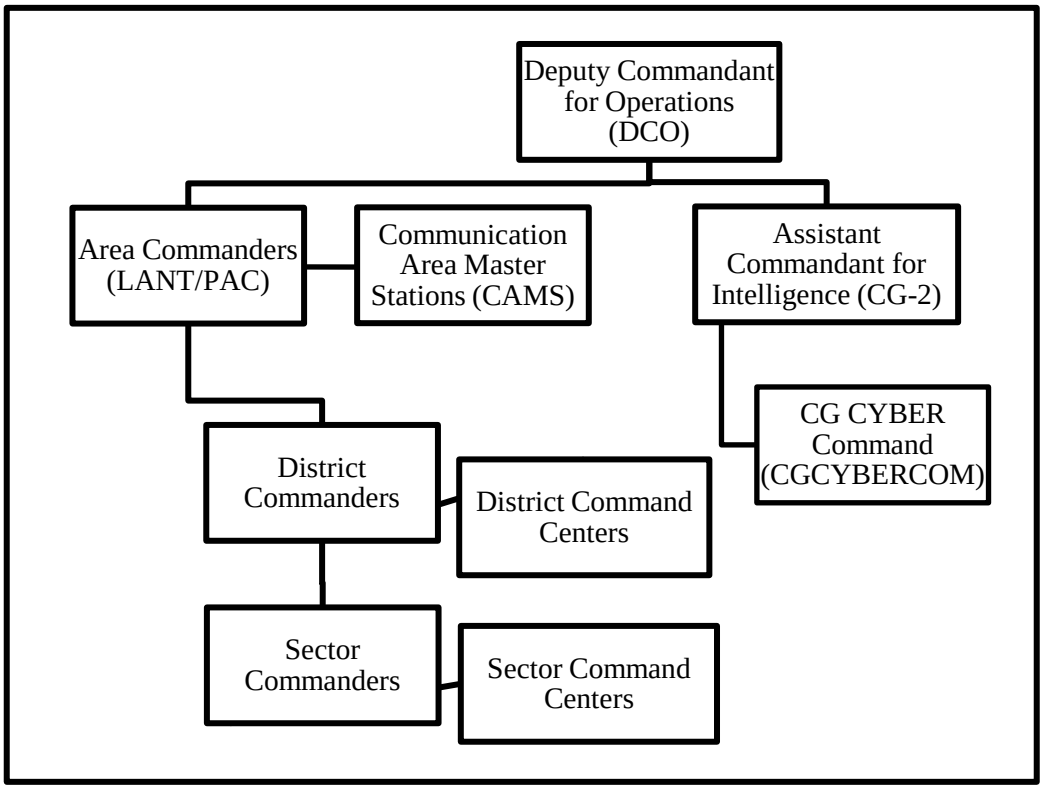
8. C4&IT System Development Life Cycle (SDLC) Roles and Responsibilities. Command, Control, Communications, Computers and Information Technology (C4&IT) System Development Life Cycle (SDLC) Policy, COMDTINST 5230.66 (series), details SDLC roles and responsibilities.

D. Telecommunications Organization. The CGTS is organized under both the Deputy Commandant for Mission Operations (DCO) and the Deputy Commandant for Mission Support (DCMS). The DCO organization uses CGTS for command and control of CG forces. The DCMS organization's role is to ensure telecommunications systems are appropriately engineered, acquired, and maintained throughout their full life-cycle. These organizations and how they relate to the CGTS are discussed in sections E and F of this Chapter.

E. Deputy Commandant for Mission Operations (DCO).

1. CGTS Command and Control Organizational Hierarchy. Command and control of the CGTS is exercised as per United States Coast Guard Regulations 1992, COMDTINST M5000.3 (series), relative to rank and command. Exhibit 1-1 below illustrates the CGTS command and control hierarchy.

Exhibit 1-1
CGTS Command and Control Organizational Hierarchy



2. Cyber Command. The mission of the CG Cyber Command (CGCYBERCOM) is to identify, protect against, and counter electromagnetic threats to the maritime interest of the United States, provide cyber capabilities that foster excellence in the execution of CG operations, support DHS cyber missions, and serve as the CG component command to United States Cyber Command. CGCYBERCOM coordinates CG enterprise network response through the Enterprise Management Facility (EMF).

3. Area Commanders. Area commanders shall exercise administrative and operational control of their communication systems (COMMSYS). This authoritative direction involves specifying and assessing the adequacy of telecommunication 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 the COMMSYS can be found in the appropriate Area Operations Plan (OPLAN).

a. The Atlantic Area (LANTAREA) Chief, C4IT Division (LANT-6) and Pacific Area (PACAREA) Chief, C4IT Division (PAC-6) are responsible for exercising operational and administrative control of the Atlantic/Pacific Area Communication System (LANTCOMMSYS/PACCOMMSYS). This includes communication area master stations (CAMS), subordinate communication stations (COMMSTAs), mobile command centers (MCC) and contingency communications caches. Additional responsibilities include operational and administrative oversight of area and district COMSEC, IA, information security (INFOSEC), personnel security (PERSEC) and physical security (PHYSEC) programs.

b. Area commanders may delegate authority to their CAMS or districts to ensure effective system responsiveness, and to:

   (1) Provide operational direction of the system components;

   (2) 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

   (3) 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 of the United States Navy (USN) and CG telecommunication systems.

c. Each area commander exercises operational and administrative control of the CGTS within their geographic area of responsibility (AOR). The area COMMSYS is subcategorized into the following facilities and services:

   (1) Communication Area Master Station (CAMS). Each area commander is supported by one of the CAMS. The CAMS acts as the area master telecommunication station providing rapid, reliable, and secure communication support to CG operational commanders and other government agencies. See Chapter 7 of this Manual for additional information on CAMS operations.

   (2) Area-Wide Communication Center (AWC). The AWC, located at each CAMS, provides record message delivery services for all shore units and CG cutters within their geographic AOR.

   (3) Communications Assist Team (CAT). Each CAMS provides CAT training and support services to cutters and other units within their geographic AOR.

(4) Communication Station (COMMSTA). COMMSTAs provide communication services that support the mission objectives of their CAMS.

(5) Contingency Communications Caches. Each CAMS operates and maintains an inventory of MCCs and portable communication assets capable of providing multi-mission and multi-agency telecommunication support during communication outages, or as a viable communication resource for DHS, and for federal, state or local law enforcement organizations during times of national emergency.

4. District Commanders. The Chief, Command, Control, Communication, Computers and Information Technology (C4IT) staff (dt), shall serve as the single point of coordination for establishing operational requirements for CG command, control, communication, computer, intelligence, sensor analysis, and data mining (C4ISM) within the district AOR. The district commander shall provide telecommunication services for the district office/district and exercise operational and administrative control of the CGTS within their geographic AOR, unless such control is assigned to the area. The district command center (CC) provides command and control of operations and assets within its jurisdiction.

5. 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 shall provide unified command and control for accomplishing CG missions and objectives. The sector command center (SCC) serves as the single point of coordination for CG operational command, control, coordination, communication, intelligence, sensor analysis, and data mining within its sector or designated AOR.

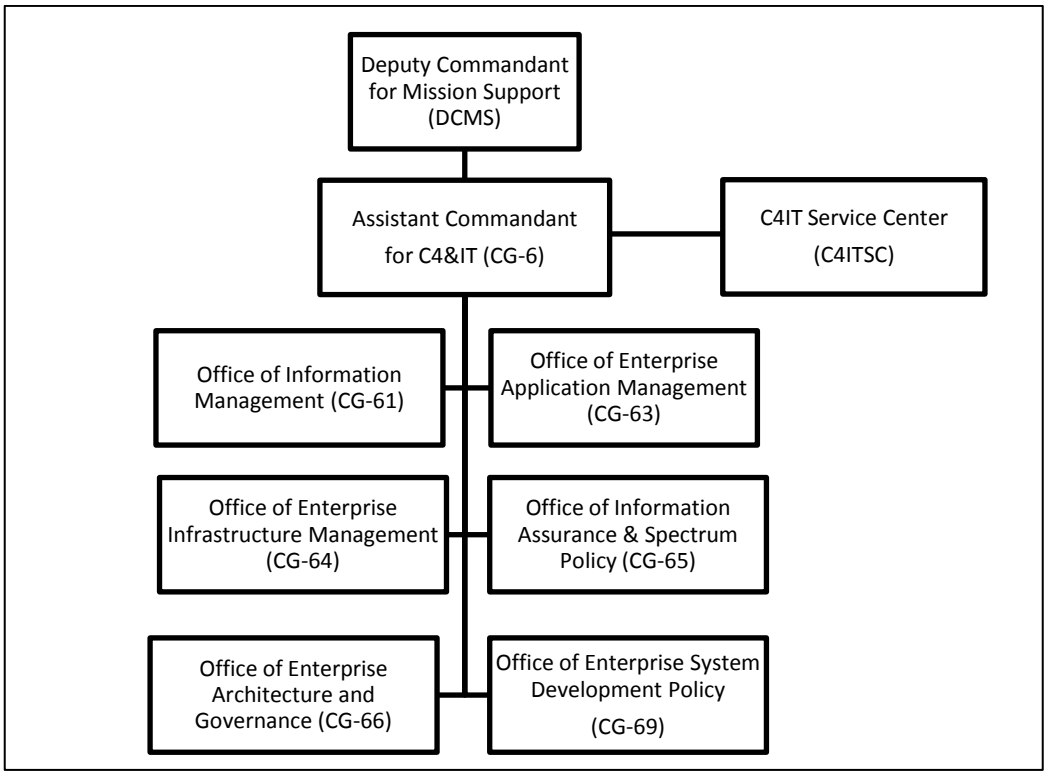
6. Communications Officer/Communications Supervisor. A communications officer or communications supervisor shall be designated at all units that maintain any type of communication watch. The communications officer or communications supervisor shall be responsible for the conduct of proper exterior communications of the command to which attached. Specific duties of the communications officer are prescribed in United States Coast Guard Regulations 1992, COMDTINST M5000.3 (series) and duties of the communications supervisor are prescribed in U.S. Coast Guard Sector Organization Manual, COMDTINST M5401.6 (series). Communications officer or communications supervisor duties shall be incorporated into Annex K to Area OPLAN, district supplement, and/or unit standard operating procedures (SOP), as applicable.

F. Deputy Commandant for Mission Support (DCMS).

1. Deputy Commandant for Mission Support (DCMS). The DCMS organization is responsible for all facets of life-cycle management for CG assets, from acquisition through decommissioning. This includes surface forces, aircraft, shore facilities and the CGTS.

a. The Assistant Commandant for C4&IT (CG-6). The mission of Commandant (CG-6) is to enhance C4&IT's value in the performance of CG missions by developing and aligning enterprise strategies, policies, and resource decisions with the CG strategic goals, mandates, and customer requirements. Specific roles and responsibilities associated with Commandant (CG-6) are listed in Command, Control, Communications, Computers and Information Technology (C4&IT) Investment Management Policy, COMDTINST 5230.71 (series).

Exhibit 1-2
Commandant (CG-6) Organization

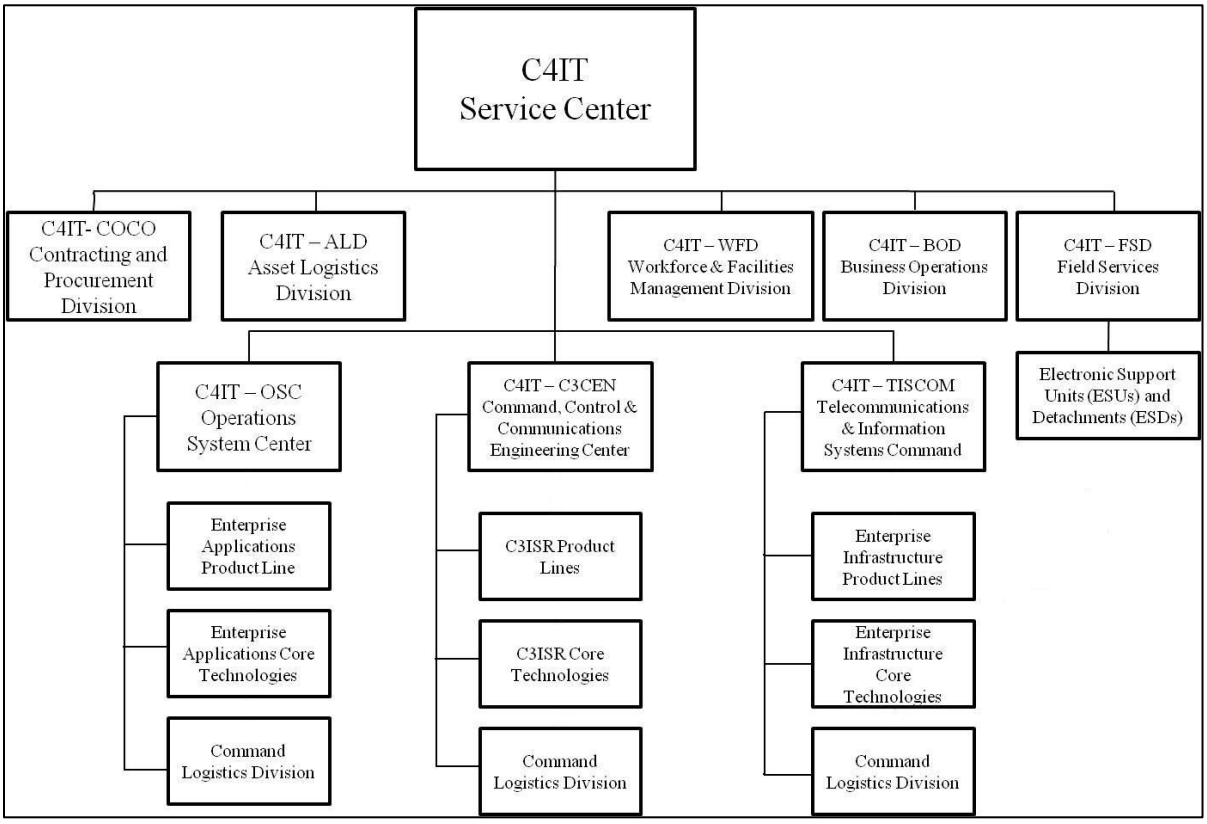


b. Office of Enterprise Infrastructure Management (CG-64). Commandant (CG-64) is responsible for establishing policy and performing centralized management of all phases of the system development life-cycle for C4IT infrastructure CG wide. The office serves as the customer interface for introduction of all new business requirements validated by Commandant (CG-761), manages enterprise architecture coordination and provides oversight for the design, development and acquisition of new infrastructure systems and operations, maintenance and enhancement of legacy systems.

c. Office of Information Assurance and Spectrum Policy (CG 65). Commandant (CG- 65) serves as program manager for the CGTS. Responsibilities include management, planning, and policy for all CG operated telecommunication systems.

d. Command, Control, Communications, Computers and Information Technology Service Center (C4ITSC). The mission of the C4ITSC is to provide full life-cycle support for CG C4&IT applications, systems and infrastructure enabling CG personnel to have the information they need to perform their jobs effectively. Additional information on the C4ITSC can be found at: https://cgportal.uscg.mil/delivery/Satellite/C4ITSC.

Exhibit 1-3
C4ITSC Organizational Hierarchy



(1) Telecommunication and Information Systems Command (C4IT-TISCOM). TISCOM provides full life-cycle support for CG C4&IT enterprise infrastructure. In addition, TISCOM operates and maintains the CG's EMF providing computer network management and network defense. TISCOM exercises administrative and

operational control of the EMF to include the Network Operations Center (NOC) and provisions for Computer Network Defense (CND).

(2) Operations Systems Center (C4IT-OSC). The OSC provides full life-cycle support for CG enterprise information systems.

(3) Command, Control and Communications Engineering Center (C4IT-C3CEN). C3CEN provides full life-cycle support for CG advanced electronic command and control, communications, and navigation systems.

(4) Field Support Delivery Elements. Electronic Support Units (ESU) and their detachments will become elements of Regional Bases as they are established.

G. Coast Guard Telecommunication System (CGTS) Relationship to Other Organizations.

1. General. The offices within the Assistant Commandant for C4&IT (CG-6) maintain formal relationships and provide liaison with international and other federal organizations impacting CGTS. These organizations include the National Telecommunications and Information Administration (NTIA), International Telecommunications Union (ITU), International Maritime Organization (IMO), International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), and the International Electrotechnical Commission (IEC). The CGTS provides the means by which the USN and a variety of law enforcement public safety agencies may communicate and remain interoperable with the CG, DHS and the Continuity Communications Managers Group (CCMG). The following sections outline some of the other relationships that support the CGTS.

2. National Communications System (NCS). The NCS was established by section 1(a) of Executive Order (EO) 12472 to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget, in the discharge of their national security emergency preparedness telecommunication functions. The NCS was transferred to DHS on 01 March 2003, as per EO 13286. The Secretary of Homeland Security (SECDHS) is designated as the Executive Agent for the NCS. The primary mission of the NCS is to ensure that federal telecommunication resources can effectively satisfy the most critical telecommunication needs of the federal government in any possible emergency situation, ranging from localized natural or man-made disasters to national emergencies, including nuclear attack. The CG participates in NCS activities and programs such as the Shared Resources (SHARES) High Frequency Radio Program and the National Emergency Communications Network (NECN). Further info may be found in the National Security and Homeland Security Presidential Directive (NSSPD) 51/Homeland Security Presidential Directive 20.

3. Defense Information Systems Agency (DISA)/Defense Communications System (DCS). DISA exercises operational control and supervision of the DCS. The respective military departments operate the component facilities. The DCS is comprised of the major portion of the individual USN, United States Army, and United States Air Force worldwide, long haul, point-to-point telecommunication facilities brought together under a single system responsive to the DOD worldwide communication needs. The C4ITSC is the principal agent for the CG.

4. 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 (DF) services when requested for search and rescue (SAR) and harmful interference cases. CG units are authorized and encouraged to coordinate with the FCC at the local level.

CHAPTER 2 COAST GUARD (CG) TELECOMMUNICATIONS GOVERNANCE AND POLICIES

A. Governance. To execute CG duties and functions, the Commandant is authorized to, among other things, establish, maintain, and operate both telephone lines and radio transmitting and receiving stations along with necessary facilities and associated equipment (14 United States Code (U.S.C.) §§ 93(a)(15) and (16)). In addition, the CG has authority to assist other federal agencies (14 U.S.C. § 141) and to cooperate with National Oceanic and Atmospheric Administration (NOAA) in collecting and disseminating weather information (14 U.S.C. § 147).

1. The Assistant Commandant for C4&IT (CG-6) is responsible for supporting all CG missions through timely delivery of telecommunications and information technology services. On the telecommunications side, CG operational and administrative communications service 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. Memoranda of Agreement and Understanding with other federal, state and local agencies.

2. In the United States, 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 47 Code of Federal Regulations (C.F.R.) § 0 et seq. (Part 80 of the C.F.R. governs public stations in the Maritime Services, 47 C.F.R. § 0 et seq). These communications are regulated by two entities: the FCC regulates public (non-federal) use of the radio spectrum and the NTIA regulates federal use of the spectrum by authority granted in the Communications Act at 47 U.S.C. § 305, through The Manual of Regulations and Procedures for Federal Radio Frequency Management. While the CG's internal use of the radio spectrum is regulated by NTIA, because the CG works closely with the maritime public, requirements placed on the public users of the spectrum by the FCC have a direct and significant impact on CG operations. Accordingly, both federal and public requirements are an integral part of the CGTS. There are numerous requirements imposed on CG operation of communication facilities, in addition to the requirements of the Communications Act and the NTIA and FCC Rules and Regulations. Some of these requirements are found in the following:

   a. International Convention for the Safety of Life at Sea (SOLAS), as amended.

      (1) Chapter IV – Radiocommunications, Regulations: 1-18 (including GMDSS).

(2) Chapter V – Safety of Navigation, Regulations. 4 - 5 requiring contracting governments to relay danger reports and to collect, examine and exchange meteorological data for the purpose of aiding navigation.

b. ITU Radio Regulations.

(1) Articles, Chapters I – IX: Chapter IX – Maritime Services.

(2) Appendices.

(3) Resolutions and Recommendations.

(4) ITU-R Recommendations incorporated by reference.

c. IEC and IALA Standards.

d. Vessel Bridge-to-Bridge Radiotelephone Act (33 U.S.C. §§ 1201-1208): USCG Regulations regarding Bridge-to-Bridge Act (33 C.F.R. §§ 26.01-26.09). This is an agreement between the United States of America and Canada for the promotion of safety on the Great Lakes by means of radio.

e. Commercial Fishing Industry Vessel Safety Act of 1988, as amended (46 U.S.C. § 2101 et seq: 46 U.S.C. §§ 4501-4588 – Applicability to certain fishing vessels).

f. 1963 Presidential Decision establishing National Communications System (NCS) – High Frequency (HF) Nets. Now under EO 12472.

g. Telecommunication Manual, COMDTINST M2000.3 (series).

h. 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).

i. Allied Communication Publication/Joint Army, Navy, Air Force Publication (ACP/JANAP).

j. Naval Telecommunications Procedures (NTP).

k. Naval Warfare Publications (NWP).

l. U.S Navy – U.S. Coast Guard Communications Policy, Office of the Chief of Naval Operations (OPNAVINST) 2000.20D.

m. Homeland Security Presidential Directive 5 (HSPD 5) – DHS/DOD Interoperability.

n. DHS National Emergency Communications Plan – DHS Interoperability.

o. DHS NSSPD 4300 (series) – Department of Homeland Security National Security Systems Policy Directives.

p. DHS Management Directive 1160.1 – DHS Operations Security (OPSEC) Program.

q. Various IA, COMSEC, OPSEC and PERSEC policies and directives concerning the security of communications, including, but not limited to, National Security Decision Directives (NSDD) and Committee on National Security Systems (CNSS) policies.

B. Telecommunications Policies.

1. General. CG telecommunication shall be conducted as per this Manual, federal requirements and policies, International Radio Regulations (IRR), treaties and international agreements, Joint and Allied/combined communication instructions, NTP's, Commandant Instructions (COMDTINST), area and district publications, and directives issued by appropriate authority. Communication publications are distributed to the appropriate CG commands as per the Directives, Publications and Reports Index (DPRI), COMDTNOTE 5600, and the COMTAC Publication Policy and Procedures Manual, COMDTINST M2600.1 (series). COMSEC publications are issued by the United States National Distribution Authority (USNDA) as per EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3.

2. New Telecommunication Service Requests. Units shall send a CG memorandum for any new telecommunication service requests via the operational chain-of-command to Commandant (CG-64) thru Commandant (CG-761), with the exception of requests for enterprise data network services (see Chapter 5 of this Manual). All new requests are subject to requirements validation by Commandant (CG-761) and final approval by Commandant (CG-64). The operational needs statement (ONS) format shall be used when submitting requests.

a. Operational Needs Statement (ONS).

(1) Problem. Clearly define the communication deficiency.

(2) Justification. State why the existing communication system established to support your organization is not able to fulfill unit requirements. State the urgency and impact of not having the requested system.

(3) System Characteristics. Describe the system characteristics including any shore infrastructure that will be used, and how it will connect to the network. Discuss the security levels provided with the equipment.

(4) Operational Concept. State how the system will be employed, how it will fill your communication deficiency, and who will be using the system.

(5) Procurement Process. State what type of equipment is being procured, who is funding it, and who is in charge of the procurement process. Indicate what procurement method will be used (e.g., General Services Administration (GSA), DISA, commercial contract).

(6) Support Requirements. Reference the Time Compliance Technical Order (TCTO) Process Guide for this installation. List the equipment that must be supported, and what mechanisms have been put in place to fund and provide the required support. Provide any information on training that will be required and how it will be provided. Provide estimated life-cycle costs (i.e., annual airtime usage, airtime cost and expected support costs).

(7) Recommendation. Recommend the course of action to resolve the shortfall.

b. All new equipment installations are subject to Surface Forces Logistics Center (SFLC) or Aviation Logistics Center (ALC) approval through the TCTO process.

C. Operational Telecommunications Policies. The following sections detail broad telecommunications policies for operations and mission support. Refer to noted applicable references as necessary for more specific information dealing with a particular policy.

1. Inter-Agency Policy. Encourage the use of CG telecommunication services by other government agencies, and promote it whenever possible. Coordinate standardized procedures and arrangements at the area and district level, with appropriate counterparts from these agencies. The requesting agency requiring telecommunication services generally is expected to reimburse the CG for any additional costs associated with the service.

2. Navy-Coast Guard Policy. Specific details can be found in U.S Navy – U.S. Coast Guard Communications Policy, OPNAVINST 2000.20D. This document outlines the role of each service, the policy for the interchange of property and services and sets forth joint doctrine to ensure effective communication system support for joint operations.

3. Inviolability of Information. The CG adheres to a policy of inviolability regarding the handling of wire or radio communication information as per the Privacy Act of 1974, 5 U.S.C. § 552a. Inviolability means that no communicated information (including organizational record messages, electronic mail (E-mail), and voice) will be released or divulged beyond the recipients intended by the originator of the information. Refer to Chapter 10 of this Manual for additional policy on official CG record messages.

a. The CG frequently intercepts communication from masters to owners reporting their vessels disabled, aground, or in a condition indicating a possible need of assistance. The CG, in the performance of its duty to protect life and property at sea and along the coast, may properly act on this information and offer the services of the CG to vessels in need of assistance. The information thus obtained and in the possession of the CG shall not be released for publication unless it is determined, as per section A.6 of this Chapter, that such information must be released.

b. Broadcast messages without designation of address are addressed to all concerned and there is no restriction on their release.

c. Personnel having a requirement to release information to audiences outside of the CGOne Network (CGOne) (e.g., CG Reserve, CG Auxiliary (AUX), public distribution) shall ensure the content is authorized for internet release. The internet refers to the CG's publicly accessible web presence available to all internet users, as well as E-mails transmitted over the CG network. Personnel are cautioned that any disclosure of Personally Identifiable Information (PII), unintended or otherwise, constitutes a privacy incident. Immediately report all discovered PII disclosures to the commanding officer and report as per Privacy Incident Response, Notification and Reporting Procedures for Personally Identifiable Information (PII), COMDTINST 5260.5 (series).

4. 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.

a. Use of Radio by United States Ships in Foreign Waters. Permission to transmit must be obtained prior to a foreign port call. A sample of a foreign port clearance record message is provided in Enclosure 3 of Foreign Port Calls, COMDTINST 3128.1 (series). The foreign port clearance record message requires specific information regarding radio requirements of the command.

b. Use of Radio by Foreign Men-of-War in United States 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.

(1) These ships must observe the radio regulations currently in effect for the area in which they are operating.

(2) Local naval commanders may withhold authorization if necessary for military reasons and must inform the Chief of Naval Operations (CNO (N3/N6)) as soon as practicable of such restrictions and provide the justification for invoking them.

(3) Foreign men-of-war must obtain frequency authorizations in advance through the USN fleet commander sponsoring the visit. If prior arrangements are not made and no USN officer is present, the senior CG officer present shall request that the cognizant fleet commander grant authorization upon arrival of visiting units.

5. Delivery of Emergency Messages to Private Vessels. The CG has no authority to handle private communication between persons ashore and commercial or private craft.

   a. If a CG unit is asked to deliver a personal message to a vessel, so advise the person making the request, with courtesy, and advise them to file the message by commercial means.

   b. The CG may relay a request for the vessel concerned to contact the marine operator for an emergency message. This service will be limited to notifying a vessel to contact a certain commercial facility for delivery, or to contact a certain person by commercial means.

6. Release of Information Acquired from Telecommunication. The requirement and procedures for the CG to furnish to the public information in its possession is set forth in United States Coast Guard Regulations 1992, COMDTINST M5000.3 (series), the Public Affairs Manual, COMDTINST M5728.2 (series), and The Coast Guard Freedom of Information (FOIA) and Privacy Acts Manual, COMDTINST M5260.3 (series).

7. Public Service Radio Broadcasts from CG Units. During a national emergency, natural disaster, or other significant events, CG units may broadcast public service information, provided such broadcasts do not interfere with the primary missions. Refer requests from the news media to Assistant Commandant for Governmental and Public Affairs (CG-0922) for approval.

8. Release of Radio Direction Finder Bearings. As per the 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), the CG will not assume responsibility for navigating a vessel, but it may provide the master of a vessel certain navigation information if available as charted or published by a reputable source. For further guidance on what information may be provided refer to the 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).

9. MINIMIZE.

   a. MINIMIZE is an operational condition declared by command authorities to clear military circuits (e.g., DOD messaging systems, E-mail, CGOne, telephone) of all nonessential traffic in an actual, simulated, or anticipated emergency. Normally, the unified commands issue the MINIMIZE order.

Designated commanders may request other commanders or friendly foreign countries to impose MINIMIZE. Commanders may also request that 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. 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 wire or radio communication passes through the telecommunication facilities of the area under MINIMIZE. Enforcing MINIMIZE is a command responsibility, and is imposed upon users, not information systems and telecommunication networks.

b. The CJCS or a commander of a unified or specified command may impose MINIMIZE upon all or part of their areas of command responsibility by general record message. These general record messages will automatically apply to CG forces in the area specified; no separate notification will be given for the CG.

c. All commanders and unit commanding officers may impose MINIMIZE within their AOR unless specifically denied by higher authority. Record messages implementing MINIMIZE shall include the applicable operational commander, area commander, district commander, and Commandant as addressees. Request for CG-wide MINIMIZE will be action to Commandant (CG-311), info to Commandant (CG-65), LANTAREA (LANT-3), and PACAREA (PAC-3).

d. When MINIMIZE is imposed upon worldwide networks, area and district commanders may authorize relaxed conditions of MINIMIZE over networks or circuits wholly within their control when in their judgment this will not adversely impact the situation requiring imposition of MINIMIZE.

e. Commands shall specifically designate a limited number of users with record message release privileges during periods of MINIMIZE.

f. Certain types of record messages are exempted from MINIMIZE to preclude interruption of important operations. Types of record messages exempted from MINIMIZE are:

   (1) Directly related to a particular mission accomplishment or operation;

   (2) Safety of life;

   (3) Critical intelligence;

   (4) Perishable weather/navigation information;

   (5) Status information or instructions pertaining to the telecommunication system affected by MINIMIZE;

   (6) Casualty Report (CASREP) record messages;

(7) Aircraft movements;

(8) Movement of fleet units;

(9) Continuing research and development (R&D) programs vital to national interest; and

(10) Serious illness, accident, or death involving CG or DOD personnel and members of their immediate families.

10. Mission Support Policies.

a. Information on mission support policies and procedures for CGTS is available through the Mission Support Handbook.

b. The Mission Support Handbook is available on line at https://collab.uscg.mil/lotus/myquickr/dcms-mission-support-organization/handbook.

c. Questions regarding information contained in the Mission Support Handbook may be directed to: AskMissionSupport@uscg.mil.

D. Destruction Devices. Information on selecting the correct destruction device for classified information, and the approved destruction methods, can be found in the Classified Information Management Program, COMDTINST M5510.23 (series).

1. Equipment approved for the destruction of classified material shall be operated properly and maintained regularly, as suggested by the manufacturer.

2. Noise must be a consideration when selecting areas within a communication facility designated for destruction (e.g., areas with installed shredders, pulverizes, pulpers). Communication spaces shall be designed to meet and comply with Occupational Safety and Health Act (OSHA) regulations for noise exposure. Refer to the Safety and Environmental Health Manual, COMDTINST M5100.47 (series) for detailed allowable noise exposure limitations.

E. Telecommunications Policy Dissemination. The Headquarters office of Commandant (CG-65), Telecommunications Plans and Policy Team maintains and disseminates this Manual. To ensure rapid dissemination of policy changes, Commandant (CG-652) issues and tracks numbered (annually by calendar year) Telecommunications Policy record messages, as necessary, between updates to this Manual. The first record message issued in a new calendar year lists the previous year's record messages which remain in effect. Current Telecommunications Policy record messages and POCs (point of contact) for Telecommunications Policy and issues may be found at:

https://collab.uscg.mil/lotus/myquickr/Telecommunications_Information/welcome.

CHAPTER 3 TELECOMMUNICATION PLANNING, REQUIREMENTS AND ACQUISITION

A. Purpose. Telecommunication planning, requirements management and acquisition oversight is necessary to ensure the CGTS remains capable of meeting the demands of CG missions and individual units remain interoperable. Enterprise-wide management of the CGTS by Commandant (CG-6) provides for the sustainment and improvement of both infrastructure and associated processes.

B. Telecommunication Planning Guidelines. Prepare and issue telecommunications directives appropriately for the organizational levels as specified below.

1. Area Telecommunication Plans. The appropriate area commander prepares and promulgates area telecommunication plans (Annex K to Area OPLAN). Annex K to Area OPLAN provides long-term policy, guidance procedures, and general information peculiar to each command is distributed to subordinate echelons. The following subject matter, as a minimum, shall be included in the Annex K to Area OPLAN:

   a. Unit(s) record message guard, drafting and releasing responsibilities;

   b. Cutter, aircraft and shore side communication;

   c. Marine Information Broadcast (MIB) schedules and special instructions;

   d. List of units and call signs;

   e. COMSEC Responsibilities;

   f. Landline circuit/network arrangements and/or configurations;

   g. Casualty reporting and restoration procedures;

   h. Procedures for requesting additional telecommunication resources and obtaining operational approval;

   i. Frequency spectrum management and frequency authorization procedures and references (http://cgweb.rss.uscg.mil/communicationsportal/Default.aspx);

   j. Emergency preparedness, contingency and continuity communication; and

   k. Interoperability with the USN, DHS, other federal, state, and local governments (i.e. land/mobile radio and first responder).

2. District Telecommunication Plans. District telecommunication plans are issued as supplements to Annex K to Area OPLANs. Requirements for content are specific to each district, but they generally follow the format of Annex K to Area OPLAN and shall satisfy requirements found in Naval Operational Planning, NWP 5-01 (series).

3. Unit Telecommunication Plans. Individual commands prepare locally-generated telecommunications plans, under the direction of the appropriate area or district commander. These plans identify administrative requirements and operational procedures unique to the unit. Duplicate material found in other publications only in the interest of continuity or completeness.

4. Preparation of a Communication Annex to Operations Order (OPORDER). An OPORDER is designed to support a particular, usually short-term, operation. The communication annex will vary in content and complexity depending upon the scope of the operation, composition of forces and communication capabilities of the participating units. Instructions for its preparation and promulgation are contained in Naval Operational Planning, NWP 5-01 (series).

5. Frequency Assignments and Approval. Per Chapter 3 and Appendix B of Spectrum Management Policy and Procedures, COMDTINST M2400.1 (series), requests for frequency assignments and modifications to assigned radio frequencies or other spectrum dependent equipment, whether for fixed or mobile use, shall be sent to Commandant (CG-652).

6. Code Plugs.

   a. The C4ITSC has the sole responsibility for developing, managing and supporting CG standard code plugs.

   b. Units are required to maintain the standard code plug in all very high frequency (VHF) and ultra high frequency (UHF) radios.

   c. Changes to the standard code plug are published by the C4ITSC via record messages.

   d. CG standard code plugs and associated encryption assignments must be appropriately handled as sensitive-but-unclassified (SBU) material and must remain internal to the CG unless specifically authorized for release by the area telecommunication staff (LANT-6/PAC-6).

   e. CG districts may authorize adding local zones of convenience to the standard code plug. District staff shall closely manage local zones of convenience to limit interoperability complications and ensure proper frequency authorizations are obtained prior to loading and use. The C4ITSC provides guidance but is not responsible for providing support for local zones of convenience.

   f. Commandant (CG-65) established CG-wide VHF and UHF standard radio frequency plans. All units with mobile and portable VHF and UHF radios (e.g., Motorola XTS-5000, EF Johnson 5100ES portable, Astro Spectra, XTL-5000) shall modify their VHF and UHF radio frequency plans and the supporting code plugs in these radios.

(1) The standard code plugs incorporate the CG-wide very high frequency/ultra high frequency (VHF/UHF) standard frequency plan. Usage restrictions and guidance for very high frequency-frequency modulated (VHF-FM) channels apply as per the VHF Radio Frequency Handbook and CG-wide Standard VHF Frequency Plan. Usage restrictions and guidance for ultra high frequency-frequency modulated (UHF-FM) channels apply as per the UHF CG-wide Standard Frequency Plan.

(2) CG district (dt) offices may authorize units in their AOR to enable the 'channel' knob on their portable tactical radios.

(3) Standard code plugs and radio frequency plans, along with the restrictions and guidance for use, and other CG tactical radio support resources are available at CG-652's tactical radio intranet site: https://cgweb.rss.uscg.mil/communicationsportal/.

(4) The current code plug hard straps all CG command and control to encryption which limits interoperability with federal and non-federal partners. The new code plug changes all CG command and control channels to selectable, which provides the necessary flexibility for interoperability but requires all tactical radio users to ensure they select encryption on radios when transmitting operational traffic over tactical command and control or CG maritime channels.

(5) Standard aviation Wulfsberg RT-5000 VHF/UHF code plug information is contained in Chapter 9 of this Manual.

C. Additional Considerations in Telecommunication Planning.

1. Communications capabilities of CG and/or other assets assigned.

2. COMSEC requirements. See Chapter 4 of this Manual.

3. Interoperability considerations with state and local law enforcement and emergency response agencies.

4. Merchant ship and recreational vessel communication capabilities vary significantly depending on vessel type, scope of operations, and intended use.

5. Communications planning and organization in response to incidents of national significance are addressed within the National Incident Management System (NIMS).

D. Telecommunication Requirements. Extensive telecommunication planning and local purchase prior to gaining operational approval and budgetary support can waste valuable CG engineering and financial resources. Initial engineering and acquisition planning in support of telecommunication projects submitted for approval shall be the

minimum necessary to provide justification and realistic best available cost estimates.

1. Operational Communications Requirements Management. The Assistant Commandant for Capability (CG-7) oversees the CG's requirements management process as outlined in Pub 7-7, Requirements Generation and Management Process. Commandant (CG-761) publishes documents outlining CG command, control, communication, computers, intelligence, surveillance, and reconnaissance (C4ISR) and telecommunications requirements.

2. Command, Control, Communications, Computer and Intelligence Baseline Architecture. U.S. Coast Guard Command, Control, Communications, Computer and Intelligence (C4I) Baseline Architecture, COMDTINST 3090.6 (series) provides a listing of operational requirements for the CG.

3. Requirements Documents. Units shall follow the procedures outlined in Chapter 2.B of this Manual for any new requests for telecommunication services. Refer to the following documents and Pub 7-7 prior to initiating any new requirements requests.

   a. C4ISR Operational Requirements Document (ORD);

   b. Long range telecommunications requirements document (under development); and

   c. Short range telecommunications requirements document (under development).

4. Engineering Changes. Requests for new telecommunication services or changes to existing services shall follow the procedures prescribed in Chapter 2, section B of this Manual.

E. Telecommunications Equipment and Services Acquisition. Acquisition and use of telecommunications equipment and services by federal agencies is subject to significant legal and regulatory restrictions.

1. Unit Procurements. Before purchasing any telecommunications equipment or services, contact district (dt) or area telecommunications staff for specific guidance. This includes, but is not limited to, telephone and cellular equipment and services, public internet services, video teleconferencing services, portable or base station radio transceivers and/or other wireless systems for the purposes of extending any network access.

2. VHF/UHF Land Mobile Radio Procurements. The standard CG VHF/UHF architecture consists of the following radios: EF Johnson 5100 Series Portable (handheld) and Motorola Series: Astro Saber, XTS-3000, XTS-5000, Astro Digital Spectra (W9), and XTL-5000. Additionally, the standard Horizon GX-1250 and Ross DSC-500 are supported with materials provisioned in the supply system and specialized projects. Units determining a need for increased VHF/UHF radio assets shall adhere to the following procedures:

a. Units with funds available for the purchase of radios to satisfy unique local requirements shall submit a request directly to the the C4ITSC and notify the chain-of-command of the purchase;

b. Units without funds available for the purchase of radios shall submit a request via the operational chain-of-command requesting funding and authorization for procurement; and

c. The C4ITSC is the only authorized procurement authority for land mobile radio procurements. The procurement and use of non-licensed or non-intrinsically safe two-way radios, such as Family Radio Services (FRS) and General Mobile Radio Service (GMRS), is not authorized for CG operational applications. No requests for approval or waiver will be considered.

3. 800 Megahertz (MHz) Radios.

a. The procurement and use of 800 MHz radios is not authorized unless the CG unit is invited by a state or local government agency for interoperability.

b. The procurement and support of 800 MHz radios needed to meet these unique local or regional interoperability requirements shall be a unit expense.

c. The CG does not support 800 MHz radios enterprise-wide for the following reasons:

(1) The federal government has no authorized spectrum in the 800 MHz band;

(2) Although many government agencies are adopting the Project-25 standard, no digital communication standard exists across all state and local agencies; and

(3) Programmatic funding is not available for expanding regional communications interoperability with local government agencies.

d. A written agreement (memorandum of agreement) shall be in place with the state or local government agency owning the 800 MHz channel/system on which the CG is planning to participate. The use of 800 MHz radios must be approved by the district (dt) C4IT office and the area office (LANT-6/PAC-6). A copy of the signed inter-agency agreement shall be forwarded to Commandant (CG-652) to facilitate enterprise-wide agency coordination.

e. There are provisions for the CG to use the non-federal 800 MHz national mutual-aid channels for regional and local interoperability provided a formal agreement has been established with the Regional Planning Committee (RPC), state or local government agency. There are 55 RPC’s that have been established by the FCC which are responsible for coordinating interoperability for their region.

f. Information on the RPC's: http://publicsafety.fcc.gov/pshs/public-safety-spectrum/800-MHz/rpc-directory.htm.

g. Use of the 800 MHz national mutual-aid channels: http://www.fcc.gov/pshs/techtopics/techtopics12.html.

h. Use of the CG's short range infrastructure, Rescue 21 (R21), for interoperability is strongly encouraged. Available interoperability frequencies can be found at: http://cgweb.rss.uscg.mil/communicationsportal.

i. It is critical to note all CG communications not intended for the general public shall, when the capability is available, be conducted via encrypted or protected channels.

F. Marine Bands. Units not yet capable of digital communications and units communicating with platforms without digital communication capabilities are authorized use of the following maritime channels in analog clear or protected mode until the requirement for analog tactical communications no longer exists. 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 21 (157.050 MHz);

3. VHF-FM Channel 23A (157.150 MHz);

4. VHF-FM Channel 81A (157.075 MHz) – Only when no other listed channel is available; and

5. VHF-FM Channel 83A (157.175 MHz) – Also used for radio-activated fog sounding device.

CHAPTER 4 COMMUNICATION SECURITY (COMSEC), COMSEC MONITORING, AND ENCRYPTION

A. Overview. The National Information Assurance (IA) Glossary (CNSS Instruction (CNSSI) 4009) defines COMSEC as "Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptographic security, transmission security, emission security (includes TEMPEST) and physical security of COMSEC material" (See COMSEC Material Control System (CMCS)). COMSEC is an integral part of IA, providing measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation.

1. The protection of government communications not intended for the general public is crucial to the effective planning and execution of CG missions. As such, all CG communications not intended for the general public, shall, when the capability is available, be conducted via encrypted channels commensurate with the classification level of the information being transmitted or received.

2. Classified information shall be processed utilizing equipment and materials approved by the National Security Agency (NSA) for classified information.

3. SBU information requiring protection such as Law Enforcement Sensitive (LE Sensitive), For Official Use Only (FOUO), Protected Critical Infrastructure Information (PCII), Sensitive Personal Identifiable Information (SPII), PII and Health Information Privacy Act (HIPA) information shall use equipment and materials approved by the NSA/DHS and/or that is National Institute of Standards and Technology/Federal Information Processing Standards (NIST/FIPS) certified. Procedures for the transmission of SBU info via CGOne network are contained in Enclosure 3 to U.S. Coast Guard Information Assurance (IA) for Unclassified Information Systems, COMDTINST 5500.13 (series).

4. When the commanding officer determines emergency action is mandatory to affect delivery, record messages of any classification may be transmitted via the lowest level cryptographically secured circuit. Additionally, under emergency conditions, information of any classification except Top Secret may be transmitted over any circuit using procedures in Communication Instructions – General, ACP 121 (series) and Allied Telecommunications Record System (ALTERS) Operating Procedures, ACP 128 (series). In such cases, the originating command shall include the following handling instruction after the classification: CLEAR TRANSEC OVERRIDE AUTH. Compromises or suspected compromises resulting from exercise of this authority shall be reported as per Classified Information Management Program, COMDTINST M5510.23 (series).

5. Commands engaged in classified or sensitive operations shall exercise great caution when communicating with the general public in response to a SAR case or similar event to prevent the release of classified or protected information.

B. Definitions.

1. Cryptographic Security. Component of COMSEC resulting from the provision [implementation] of technically sound cryptographic systems and their proper use. This component deals with the actual encryption of information.

2. Cryptographic Systems. Associated information assurance items interacting to provide a single means of encryption or decryption (See Information System below).

3. Transmission Security (TRANSEC). Measures (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.

4. 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)

5. Emission Control (EMCON). EMCON is one procedure used to provide TRANSEC by means of control of all electromagnetic and acoustic radiations, including communication, radar, electronic warfare (EW), and sonar. During EMCON imposition, no electronic emitting device within designated bands, including personal communication devices, will be operated unless absolutely essential to the mission. Refer to Fleet Communications, NTP 4 (series) for more information regarding EMCON.

6. TEMPEST. A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. TEMPEST policy is contained in U.S. Coast Guard TEMPEST Program, COMDTINST M2241.6 (series). During the initial secure communication planning stages, the C4ITSC (BOD-IAB) shall be contacted for the latest TEMPEST requirements.

7. Communication Security (COMSEC) Material. Item designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to key, equipment, devices, documents, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.

8. COMSEC Material Control System (CMCS). Logistics and accounting system through which COMSEC material marked “CRYPTO” is distributed, controlled and safeguarded. Included are the COMSEC central offices of record, crypto logistic depots and COMSEC accounts. COMSEC material other than key may be handled through the CMCS (See Electronic Key Management System (EKMS) definition).

9. Electronic Key Management System (EKMS). A component of the CMCS which is an interoperable collection of systems developed by services and agencies of the United States Government to automate the planning, ordering, generating, distributing, storing, filling, using, and destruction of electronic key and management of other types of COMSEC material. CG implementation of the EKMS is contained in Appendix A of this Manual.

10. Communications Tactical (COMTAC) Publications. COMTAC publications contain telecommunication, tactical, and procedural doctrine within a system of accountability which provides for the physical security of these publications. Detailed guidance for maintaining a COMTAC library is contained in the COMTAC Publication Policy and Procedures Manual, COMDTINST M2600.1 (series).

11. 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.

12. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

13. Information System. A discreet set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

C. Classified Information Management Program. These are the measures designed to prevent unauthorized access to non-COMSEC classified equipment, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft. This program is under the cognizance of Commandant (CG-DCMS-34). Refer to the Classified Information Management Program, COMDTINST M5510.23 (series) for details.

1. Personal Security (PERSEC) and Suitability Program. Physical security begins with properly cleared personnel that handle national security information and related systems. Guidance concerning PERSEC and suitability is found in the Personnel Security and Suitability Program, COMDTINST M5520.12 (series).

2. Telecommunication Facility Security. Physical security is achieved within CG telecommunication facilities through guidelines promulgated in Physical Security and Force Protection Program, COMDTINST M5530.1 (series), and EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3.

D. Other Classified Material Control (CMC) Systems. The physical handling and storage of certain classified material falls under a CMC system per the Classified

Information Management Program, COMDTINST M5510.23 (series) to include the following material:

1. All Top Secret information;
2. Sensitive Compartmented Information (SCI);
3. COMTAC information; and
4. Classified North Atlantic Treaty Organization (NATO) material.

E. Communication Security (COMSEC) and Information Assurance (IA) Responsibilities. The following are specific roles and responsibilities that govern overall COMSEC and IA protecting classified and SBU government communication:

1. 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 NIST, is responsible for overall policy regarding the safeguarding of SBU including SBU National Security Information (NSI) and the associated information security systems.
2. Secretary of Defense (SECDEF). SECDEF, assisted by the NSA, is responsible for the protection of classified NSI and the associated IS Systems.
3. Director of National Intelligence (DNI). DNI is responsible for intelligence related information and systems.
4. Secretary, Department of Homeland Security (SECDHS). SECDHS is responsible for protection of classified or SBU information on all department information systems as directed by OMB or SECDEF.
5. Commandant (CG-65). Commandant (CG-65) has overall COMSEC responsibility for the CG.
6. Command, Control, Communications, Computers and Information Technology Service Center (C4ITSC). C4ITSC (BOD-IAB) serves as the principle agent, under direction of Commandant (CG-65), for COMSEC matters throughout the CG.
    a. The C4ITSC (BOD-IAB) shall be responsible for updating and issuing, in coordination with Commandant (CG-65), COMSEC policy requirements throughout the CG.
    b. The C4ITSC (BOD-IAB) promulgates detailed CG COMSEC policy and exercises service-wide management and oversight of CG EKMS accounts.

Additional information on EKMS roles and responsibilities is available in Appendix A of this Manual.

c. The C4ITSC 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.

d. C4ITSC (BOD-IAB) also functions as the CG Command Authority for modern key under the EKMS Central Facility and acts as the Controlling Authority for all CG controlled keys, including those comprising the national level Joint Inter-Agency Counterdrug COMSEC (JIACC) Keying Material (KEYMAT) Package.

7. Area Commanders. Area commanders shall assist in the management of the CG COMSEC program as follows:

a. Provide oversight and management of area COMSEC matters and physical security measures as per applicable instructions;

b. Provide oversight and management of the EKMS program within their AOR as per procedures outlined in Appendix A of this Manual;

c. Area commanders are authorized to request and approve COMSEC monitoring within their AOR. Area commanders are responsible for making maximum use of the information provided by the monitoring agency as best as they are able toward general OPSEC/COMSEC training and awareness within their AOR. Area commanders, or those individuals acting in these capacities, must personally request and approve COMSEC monitoring within their AOR. This authority may not be re-delegated; and

d. Review of COMSEC monitoring reports:

(1) Regularly review and evaluate breaches in COMSEC for impact on overall operations,

(2) Report significant COMSEC disclosures observed in these provided reports as per section G of this Chapter, and

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

8. District Commanders. District commanders shall direct their units as per area COMSEC instructions, and address their COMSEC and COMSEC monitoring needs to the cognizant area commander.

a. Provide oversight and management of COMSEC measures as per applicable instructions.

b. Provide oversight and management of the EKMS program within the AOR as per procedures outlined in Appendix A of this Manual.

c. Review of COMSEC monitoring reports.

d. Regularly review and evaluate breaches in COMSEC for impact on overall operations.

e. Report significant COMSEC disclosures observed in these provided reports as per section G of this Chapter.

f. Identify and initiate corrective administrative actions as necessary.

9. Commanding Officers. Commanding officers are responsible for maintaining a comprehensive COMSEC program at their commands. Unit commanding officers are responsible for the manner in which their personnel perform EKMS/COMSEC duties. At a minimum, commanding officers shall:

a. Provide oversight and management of COMSEC measures as per applicable instructions;

b. Be thoroughly familiar and comply with the specific responsibilities and duties and required inspections as outlined in Chapter 4, Article 450 of EKMS 1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3 (See Appendix A);

c. Conduct personnel training which 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;

d. Regularly review and evaluate breaches in COMSEC for impact on local and overall operations; and

e. Identify and initiate corrective administrative actions as necessary in response to COMSEC incidents.

F. Communication Security (COMSEC) Monitoring. COMSEC monitoring is a means by which unauthorized disclosures of classified and SBU government information on non-secure telecommunication circuits and systems may be detected and brought to the attention of the agency being monitored. The information provided by the monitoring agency is to assist in identifying trends, vulnerabilities and weaknesses. It is not meant for punitive action. Awareness of active COMSEC monitoring of government telecommunication systems is an essential element of deterrence of such disclosures. National Telecommunications and Information Systems Security Directive Number 600 (NTISSD No. 600) is the controlling directive for COMSEC monitoring of government telecommunication systems. Commandant (CG-65) is the overall program office for all aspects of CG COMSEC monitoring. Commandant (CG-65) also maintains a primary and alternate CG POC with the monitoring agency for the express purpose of addressing specific legal and operational issues that may arise from time to time.

1. Purpose. This section outlines certain responsibilities of area and district commanders and their legal officers in carrying out the requirements of NTISSD No. 600.

2. Definitions. NTISSD No. 600 contains a complete list of applicable definitions. However, the following definitions as applicable to COMSEC monitoring are provided:

   a. COMSEC monitoring. The act of listening to, copying, or recording transmissions of one's own official telecommunications to analyze the degree of security.

   b. Telecommunications. Preparation, transmission, communication, or related processing of information (writing, images, sounds or other data) by the transmission, communication, preparation or processing of information by electrical, electromagnetic, electromechanical, electro-optical or electronic means.

   c. OPSEC. OPSEC is a systematic and proved process by which the United States government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive government activities.

3. Policy. All COMSEC monitoring by the CG or as mutually agreed upon by the CG and another agency, shall be conducted in strict compliance with NTISSD No. 600 and this section.

   a. Official government telecommunication and computer systems (including specific CG communications circuits) are subject to COMSEC monitoring at all times, and the use of such communication systems constitutes consent to COMSEC monitoring as described in Limited Personal Use of Government Office Equipment and Services, COMDTINST 5375.1 (series).

   b. With limited exception, no agency may monitor CG telecommunication for COMSEC purposes without the express written approval of the Commandant.

4. Procedures for Legal Certification. Commandant (CG-65) ensures all the legal provisions of NTISSD No. 600 are met, reviewed and recertified every 2 years with applicable monitoring agencies. Users of government telecommunication systems must be notified in advance, as per the guidelines below, that their use of these systems constitutes consent to monitoring for COMSEC purposes. As such, the area legal offices shall annually, or when requested by Commandant (CG-65), conduct a legal review of current COMSEC monitoring procedures and shall ensure at least one of the following list of mandatory methods for COMSEC notification are in place at each unit within their AOR. When completed, the area legal office shall notify Commandant (CG-65) to certify that the provisions of NTISSD No. 600 are met (official E-mail will suffice). Commandant (CG-65)

will then ensure the CG is recertified so monitoring agencies may, if applicable, legally continue to provide COMSEC monitoring for the CG.

a. Notice of the existence of COMSEC monitoring can be accomplished by any of the following means or any combination thereof so long as the appropriate area legal officer considers the means chosen to be legally sufficient to achieve proper notification in terms of content, prominence, and specificity:

(1) Decals placed on the transmitting or receiving devices;

(2) A notice in the daily bulletin, plan of the day, or similar medium;

(3) A specific memorandum to users;

(4) A statement on the cover of the official telephone book or communication directory; and

(5) A statement in the standard operating procedures, communication-electronics operating instructions, or similar documents.

b. Certification of the means chosen to achieve proper notification in terms of content, prominence, and specificity is accomplished by a written certification by the appropriate area legal officer, as authorized by the Judge Advocate General (JAG), to the agency duly authorized and approved to conduct COMSEC monitoring of CG users of government telecommunication systems. The following format is suggested:

"The (insert appropriate area) legal officer, as authorized by the Judge Advocate General of the Coast Guard, certifies that the following means (please list) provided legally sufficient and proper notice in terms of content, prominence, and specificity to United States Coast Guard users of government telecommunication systems that their use of such systems constitutes implied consent to communication security (COMSEC) monitoring."

G. Unauthorized Disclosure. A unauthorized disclosure is any classified, SBU, PII items listed is the CG Critical Information List (CIL), or Essential Elements of Friendly Information (EEFI) list or material that has been transmitted via an unauthorized method resulting in a possible exposure of that information or material to unauthorized individuals. Immediately report all discovered disclosures to minimize the risk of exposure. It is imperative that commands continually educate their personnel on how to avoid disclosures, what to do if one is discovered and who to contact. COMSEC monitoring reports should be considered a source of unauthorized disclosures and mitigated when possible. The Coast Guard Computer Incident Response Team (CGCIRT) has the primary responsibility for reporting and acting on all reported computer related classified, SBU/FOUO (to include CIL and EEFI items) and PII disclosures contained in these reports. Commandant (CG-65) shall be copied on all CGCIRT reporting. Specific reporting requirements are as follows:

1. Classified information and material disclosure reporting shall be as per the CG Classified Information Management Program, COMDTINST M5510.23 (series). Specifically the unit command security officer (CSO), information system security officer (ISSO) and custodian of the information shall immediately be notified. Disclosures involving a computer shall be reported to the CGCIRT. Include Commandant (CG-DCMS-34) for all classified information reporting, Commandant (CG-2) for all intelligence (INTEL) related information reporting regardless of classification and Commandant (CG-65) for all reporting involving CG networks;

2. SBU disclosures shall be reported locally to the CSO/ISSO and the CGCIRT if the disclosure involves a CG computer; and

3. Compromise or loss of information containing PII is considered a privacy incident and shall be immediately reported to the unit commanding officer upon discovery as per the Privacy Incident Response, Notification and Reporting Procedures for Personally Identifiable Information (PII), COMDTINST 5260.5 (series). The CGCIRT shall be notified if the disclosure involves a CG computer.

H. Advanced Encryption Standard (AES). CG units shall use AES (256 bit) encryption as the primary encryption mode for operational communications. Data Encryption Standard (DES) shall be maintained in all VHF/UHF radios until further notice. This provides for backward compatibility for unique non-AES encryption requirements.

1. CG units participating in multi-agency operations or working with other CG units without AES encryption may use DES encryption, as required, for communication interoperability.

2. AES KEYMAT shall be obtained from Customs and Border Protection (CBP) National Law Enforcement Communications Center (NLECC), Orlando, Florida. The encryption key shall be obtained via over-the-air-rekeying (OTAR) or manual dial-in procedures. Units are authorized direct liaison with CBP NLECC for OTAR and Key Management Facility (KMF) services and support.

CHAPTER 5 TELEPHONE, NETWORK, AND SATELLITE TELECOMMUNICATIONS SERVICES

A. General. The CGTS includes owned and leased circuits, channels, services and equipment that provide data, voice, and video networks throughout the CG. The following sections define systems and detail policies pertaining to telephone, network and satellite communication services operations, provisioning and maintenance.

B. Network Oversight Functions. The C4ITSC is responsible for the engineering, documentation, and implementation of the CG telecommunication and information systems infrastructure. The C4ITSC provides oversight for the following CG telephone, network and commercial telecommunications services:

1. Federal telephone services (FTS) contracts. The C4ITSC administers FTS contracts including: Networx (formerly Federal Telecommunications System 2001) and GSA niche telecommunication contracts such as WITS3 (Washington Interagency Telecommunications System), International Direct Distance Dialing (ID3), Federal Wireless Telecommunications Services (FWTS), electronic commerce, internet access, E-mail, etc;

2. CGOne and GuardianNet;

3. All commercial satellite communication (COMSATCOM) services (e.g., Inmarsat Fleet Broadband, Ku-band) and associated contracts;

4. All DISA, Joint Staff, DOD, or other Department or Agency controlled services. These include Secret Internet Protocol Router Network (SIPRNET), Non-Classified Internet Protocol Router Network (NIPRNET), Inmarsat, Enhanced Mobile Satellite Service (EMSS), and Defense Switch Network (DSN);

5. Any inter-agency service provided to CG units (e.g., National Weather Service (NWS)) for special organization-wide networks;

6. All data and voice system encryption devices (see Chapter 4 and Appendix A of this Manual);

7. The C4ITSC administers the telecommunication line and terminal facilities/services for all units and provides technical assistance as needed by local servicing personnel. Services and circuits include the following:

   a. Local telecommunication services for all units to include wireless systems as per Use of Unclassified Wireless Devices, Services, and Technologies, COMDTINST 2010.2 (series); and

   b. Procurement of telephone service contracts for customer provided equipment.

      Note: Commanding officers of Headquarters units shall control telecommunication facilities at their units. C4ITSC shall provide requisite technical assistance to units with permanent telecommunication support staffs

via support agreements coordinated between the Headquarters unit, its servicing Base Support Unit (BSU), and the C4ITSC.

C. Policy.

1. Designated agency representatives (DAR) are field representatives assigned to BSU/ESUs and other designated commands authorized and trained to commit funds for telecommunication services. CG DARs are the only authorized agents allowed to place orders for telecommunication circuits and services (excluding cellular wireless) from approved sources and shall use the most current policy and practices promulgated by the C4ITSC. DAR authority is restricted, limited and managed by the DAR administrator at the C4ITSC. Per Department of Homeland Security Management Directive System MD 4800, DARs shall be designated in writing by the agency DAR administrator and certified as contracting officers technical representatives (COTR).

2. Voice Systems.

   a. Long distance telephone networks shall not be used for data transmissions (except for secure and non-secure facsimile (FAX). Requests for waivers from this policy shall be submitted in writing with supporting rationale to Commandant (CG-65).

   b. Requests for voice DCS services (e.g., DSN) from DISA, Joint Staff, DOD, or other department or agency service, or for service changes, shall be submitted in writing with supporting rationale to the C4ITSC.

   c. DSN services are not authorized for CG AUX members.

   d. 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 C4ITSC. Units requesting toll-free service will be responsible for charges incurred by the service.

3. Non-Appropriated Funds Activity (NAFA). Government funded local telephone or Networx service may be provided to NAFA facilities but it is restricted to NAFA officers in performance of their assigned military duties only. Procuring services from federal contracts (e.g. Networx) for routine NAFA business is limited to services that can be established to directly-bill to the facility.

   a. Pay telephone service shall be contracted between:

      (1) The CG and the telephone company, with commissions deposited in the general fund of the Treasury as miscellaneous receipts; or

      (2) NAFA facilities and the telephone company, with commissions retained by the NAFA facility. Refer to the Accounting Manual, COMDTINST M7300.4 (series).

b. Government funded local telephone or Networx services are not authorized for CG Credit Unions.

c. Local telephone or Networx services paid for with appropriated funds are not authorized for installation in residences. Government owned/leased representational facilities are exempt from this restriction. Appropriated funds may be used to install, repair, and maintain telephone circuits and wiring in CG flag officer residences owned or leased by the United States government and, if necessary, for national defense purposes. This exception is for the installation of secure telephone equipment (STE) in support of the Maritime Defense Zone mission and national security. Commandant (CG-6) must approve this service with concurrence from the DHS.

4. Federal Telephone Services (FTS) Contracts. Basic FTS service includes inter-local access and transport area (LATA) switched voice service for official government long distance service. Inter-LATA is defined as telecommunication services that originate in one LATA, and terminate in another LATA.

a. All units requesting FTS services shall coordinate requests with their servicing DAR.

b. Units needing non-standard FTS services must route the service request, in writing, to the C4ITSC via their local servicing DAR. The primary source of funding for many of these services shall be direct billing to account strings. If direct billing does not meet accounting circumstances, then use central billing for the services and services will be billed back annually. Non-standard services found on current federal contracts include:

(1) Enhanced switched voice (e.g., federal calling cards, toll-free service and audio teleconferencing);

(2) Switched data services (e.g., Integrated Services Digital Network (ISDN), Switched 56kb);

(3) Packet Switched Services (e.g., frame relay, dedicated access, or dial-up access);

(4) Video transmission service (wide-band video transmission service (full motion) switched video); and

(5) Internet protocol (IP)-based services (e.g. IP service, voice over internet protocol (VoIP), digital subscriber line (DSL)).

c. TISCOM shall act as the enterprise federal calling card manager for federal calling cards with local management delegated to a unit-designated federal calling card administrator. The enterprise federal calling card manager shall issue federal calling cards per the most current CG Networx DAR guidelines. Unit calling card administrators shall locally manage calling card inventory for their unit, notifying TISCOM of changes in card requirements (i.e.

personnel transfers), requests for new cards, and inventory validation. Federal calling cards for units requiring international dialing capability in the performance of their official duties shall be directly-billed to the unit. Government Emergency Telecommunications Service (GETS) cards are not federal calling cards and are discussed later in this Chapter.

(1) Federal calling cards will not be issued for non-government business.

(2) Prepaid calling cards (i.e. non-federal calling cards) must be ordered using the government international merchant purchase authorization card (IMPAC).

(3) Use of prepaid calling cards with air phones (commercial airlines) and rail phones (commercial railways) is strictly prohibited.

(4) The federal calling card is authorized for official use while telecommuting. It will not be used to place personal telephone calls even if the user intends to reimburse the government.

(5) CG Reservists are authorized to use federal calling cards only while preparing or arranging for active duty and while in an active duty status.

(6) CG AUX personnel are not authorized federal calling cards.

5. Facsimile (FAX). FAX may be used for any level of correspondence between CG commands where timely service is required. However, FAX does not provide the users with any level of security unless a secure FAX configuration is used. As specified in the DHS Management Directive 11042, "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 FAX 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." If specific guidance on FAX is needed, individual commands shall check with their area or district C4IT division.

a. Secure FAX. The term "secure facsimile" refers to a combination of a STE and a FAX machine which meets the standards outlined in the U.S. Coast Guard TEMPEST Program, COMDTINST M2241.6 (series). Minimum security requirements for the handling and control of STE terminal equipment and associated KEYMAT can be found in Annexes AB and AC of EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3.

b. Security. 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 that are sent or received via secure FAX. Specific guidance can be found in Chapter 5 of EKMS 1 (series) EKMS Policy and Procedures for Navy

Electronic Key Management System Tiers 2 & 3 and the Classified Information Management Program, COMDTINST M5510.23 (series).

c. Accountability. Record messages sent via FAX must be properly released by command authority, assigned a date-time group and entered into the telecommunication system. This will ensure proper filing and accountability, and will prevent duplication of date-time groups. Proper file accountability shall be per Chapter 6 of this Manual.

6. Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS).

a. The GETS/WPS program is sponsored by NCS and is not a service provided by the Networx contract. The C4ITSC acts as the lead systems support agent (SSA) and program manager, while ordering and inventory management is delegated to ESU Program Administrators (who may or may not be a DAR).

b. GETS provides priority telephone call routing, allowing units to complete emergency calls when telephone circuits are overloaded. GETS cards are not federal calling cards. GETS provides access only where an existing telephone infrastructure (dial tone) exists and only expedites completion of calls through priority handling of the call through the Public Switched Telephone Network (PSTN). GETS calls do not preempt calls in progress or deny the general public use of the PSTN.

c. Users should always try to complete the call by normal means, and then use the GETS card if circuits are busy.

d. WPS was developed to provide priority treatment for emergency calls made from cellular phones. CG policy is to provide WPS for government provided cellular phones only.

e. WPS is a service very similar to the terrestrial based GETS system. It is a method of improving connection capabilities for a limited number of authorized cell phone users. In the event of congestion in the wireless network, an emergency call using WPS will have priority in the queue for the next available channel. WPS calls do not preempt calls in progress or deny the general public use of the radio spectrum.

f. To request GETS or WPS service, contact your GETS/WPS program administrator. Program administrators will provide enrollment forms and further detailed instructions on how GETS/WPS service will be started on your phone.

7. Pagers. The area or district commander may operationally approve paging equipment for CG personnel.

a. Paging service should be leased.

b. Costs for the leasing of paging equipment and service shall be borne by the unit using them.

8. Cellular Telephones. Unit commanding officers, officers-in-charge and office chiefs are permitted to procure cellular equipment and usage services as required. Unconstrained use can result in excessive equipment procurement and on-air costs. Units closely monitor cellular telephone use and shall establish local policies and procedures for effective management and oversight of locally acquired cellular equipment and services.

   a. Cellular systems do not provide COMSEC unless they use a global security module (GSM-SM) for mobile communication security.

   b. Requests for cellular secure telephone modules shall be forwarded to Commandant (CG-64) via the appropriate area or district commander.

   c. Cellular phone management, life-cycle costs and usage fees shall be borne by the unit incurring them.

9. Point-to-Point Wireless Services. Wireless transmission services (i.e., microwave or satellite) will be coordinated and funded by the local unit and their regional telecommunication managers. The C4ITSC will provide support in identifying advantageous service-wide contracts to implement this new technology. Wireless service may be used in lieu of telephone lines as follows:

   a. During telephone circuit failures;

   b. When telephone service to isolated locations is not available or practical;

   c. For short, limited-range point-to-point wireless links connected to telecommunication channels;

   d. Where wireless service would provide superior service at reduced cost as opposed to wired solutions;

   e. When the operating environment dictates use of wireless services to best facilitate mission success; and

   f. Contingency communications in support of continuity of operations (COOP) to the extent of operational infrastructure.

10. Participation in Federal, State, or Local Wireless Voice Networks. The following policies and options are approved for participation in wireless networks:

   a. Use a common frequency already authorized for both the CG and federal, state and local partners. Some agencies use common radio bands supported by CG equipment, such as VHF/UHF and VHF Marine bands. Marine band use shall be per Spectrum Management Policy and Procedures, COMDTINST M2400.1 (series). Any use of CG frequencies by non-government agencies

shall be authorized in writing and shall only be used for communication with CG units.

b. Public Safety Bands (700/800 MHz). CG use of public safety frequency license must be certified as necessary in writing by local partners per Spectrum Management Policy and Procedures, COMDTINST M2400.1 (series).

c. Use of a radio provided by federal, state or local agency or procured compatible radio (handheld or mobile). The following provisions apply for this option:

(1) Cutters. Follow TCTO process for installations.

(2) Standard Small Boats. Follow the TCTO process for installations. Options in sections 9.a and 9.b, of this Chapter, and handheld radios (provided by other government agency or purchased) are authorized until a CG-wide solution for small boats is identified.

(3) Non-standard Small Boats. As approved by district boat manager.

(4) Shore Units. Follow the TCTO process for installations.

d. Units shall use a gateway to connect a CG communications asset (e.g., R21, HF, VHF, UHF) to a federal, state or local agency's interoperability system (Integrated Wireless Network (IWN), Enterprise Land Mobile Radio (ELMR), 800 MHz, HF/VHF, trunked or conventional). Connection may be made permanently or on an as-needed basis.

e. Units shall notify their district spectrum manager, for further coordination with district (dt), prior to adding new frequencies to code plugs, authorizing additional users to current CG frequency authorizations, or using another agencies radio frequency.

f. Units shall notify Commandant (CG-652 /CG-64), and LANT-6/PAC-6 as appropriate, of such participation, procurement and installation via their chain-of-command.

11. Directory Listing. To minimize delay in reporting distress cases, adequate directory listings with correct telephone numbers shall be arranged with local telephone companies. Units are responsible to ensure their local telephone company's directory list managers are providing the information necessary to keep their listings current.

a. Directories should include area, district, and sector command centers in that particular locality.

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.

12. Emergency Telephone Number 911. The emergency telephone number 911 has been designated nationally for public use in reporting emergencies and requesting emergency services. The responsibility for establishing a 911 program resides with local government.

    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.

    c. Funding requirements shall be identified at the district level.

13. Caller Identification (ID). Caller ID services shall be provided to the greatest extent possible to all operational CG units as a deterrent to fraudulent distress calls. Switchboards and services ordered for these units shall be capable of providing Caller ID and automated number identification services as standard features.

D. Private Branch Exchange (PBX), Voice over Internet Protocol (VOIP), Unified Communications (UC), and Video Teleconferencing Systems (VTC). Telephone communication requirements include:

1. Commercial telephone service via leased or owned switching equipment. This is applicable to all existing and future CG facilities, ship and shore, requiring telephony voice, data, video and peripheral equipment products and services;

2. Long distance access. Dedicated lines or central exchange access provided by GSA or the CG are preferred. If physical access is not available, federal calling cards should be used;

3. Continuous recorded monitoring of critical telephone circuits, as required, to document verbal agreements and pertinent information exchanges. Such recordings constitute permanent records that may be significant evidence in criminal or civil liability assessments, and enable reconstruction of events during emergency response activities. This includes the archival capabilities and specifications;

4. Voice circuits as necessary for rapid coordination with other local operating units and/or agencies; and

5. Telephone answering devices to automatically disseminate or receive information in a "hands off" mode (i.e., Automated Attendants and Interactive Voice Response).

6. Additional policy and guidance is located on the CG-642 Telecommunication Systems Division portal site (Telephony Systems and Peripheral Equipment document): https://cgportal.uscg.mil/lotus/myquickr/telecommunications-systems-division.

E. Telephone and Circuit Management.

1. Telephone Management Programs. The Telephone Management Program shall be administered by the C4ITSC. Local programs shall be implemented and administered by servicing BSU/ESU. Local programs shall 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 E.2 of this Chapter;

   b. Personnel responsible for procuring and managing telephone service (DARs) are familiar with and comply with applicable Federal Management Regulations (FMR) and Federal Acquisition Regulations (FAR). An annual inventory of all installed telephone station equipment and features is conducted and used to certify the accuracy of the statements of charges. All unnecessary equipment and features are removed;

   c. An acceptable standard grade of service is maintained:

      (1) A station line denial rate of five calls in 100 (P05) during the normal busy hour is the acceptable standard grade of service,

      (2) The Networx contract provides seven calls in 100 (P07) blockage; and

   d. Where practical, consolidated or common user systems are used to provide service to multiple CG units.

      Note: Unapproved Area Codes. Software blocks to unapproved area codes (e.g., 900) shall be programmed whenever possible on CG owned/leased telephone systems.

2. Personal Use of Government Office Equipment. Current policies regarding authorized, inappropriate, and prohibited uses of CG office equipment are outlined in Limited Personal Use of Government Office Equipment and Services, COMDTINST 5375.1 (series). Commands are authorized to approve additional personal use on a case-by-case basis. The following policies apply to personal use of government telephone systems:

   a. 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 for a basic service charge. Each local call is billed. CG members and employees may place the following types of local and/or long distance calls using commercial/dial 9 (or 8) access 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 placed during working hours such as a local government agency or physician; and

(5) Calls to arrange for emergency repair to a home or automobile; or certified in advance by the employee's/member's supervisor as official.

b. Long Distance Calls. All other long distance calls not related to assigned duties that must be made during normal working hours shall 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; and

(4) Collect.

c. Requirements for All Calls. All calls both local and long distance placed under the provisions of the following policy:

(1) Must not adversely affect an individual's or someone else's performance of official duties;

(2) Must be of reasonable duration and frequency; and

(3) Could not have been made during non-working hours.

3. Intra-Area Circuit. The C4ITSC and ESU DARs shall maintain records of all intra-area dedicated circuits. These records shall include, at a minimum, the following:

a. Circuit number;

b. Carrier identification (if CG owned, so indicate);

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); and

g. Monthly recurring cost of the circuit.

F. Telecommunication Networks. CG commands are connected via a wide variety of data networks public, unclassified and secure. Data networks are administered and provisioned by the C4ITSC and serviced by local BSU/ESU personnel.

1. Definitions.

   a. Local Area Network (LAN). A LAN supplies networking capability to a group of computers in close proximity to each other, such as in an office building. A LAN is useful for sharing resources like files, printers, games or other applications. A LAN in turn often connects to other LANs, and to the internet or other wide area network (WAN).

   b. Wide Area Network (WAN). A WAN spans a large geographic area, such as a state, province or country. WANs often connect multiple smaller networks, such as LANs.

2. Coast Guard (CG) Networks.

   a. Department of Homeland Security (DHS) OneNet. DHS OneNet is the WAN for DHS. DHS OneNet is a multi-protocol label switching (MPLS) network.

   b. CGOne (Coast Guard One Network). CG implementation of DHS OneNet.

      (1) The C4ITSC monitors the network on a 24/7 basis.

      (2) CGOne provides CG units access to the internet.

   c. Internet. The internet is a publically accessible (non-secure) global system of interconnected computer networks that use the standard internet protocol suite, TCP/IP, to serve billions of users worldwide. Commercial or “dirty” internet connections are subscription services that do not pass through CG/DHS Trusted Internet Connection (TIC). Refer to Enclosure (3) of U.S. Coast Guard Information Assurance (IA) for Unclassified Information Systems, COMDTINST 5500.13 (series) for additional policies and guidance on the installation and use of commercially provided internet services at CG facilities.

   d. Secret Internet Protocol Router Network (SIPRNET). SIPRNET is an enterprise administered WAN that operates at the Secret/Not Releasable to Foreign Nationals (Secret/NOFORN) classification level and is also authorized to process NATO Secret and below information. SIPRNET operates in a manner similar to the internet, but as a secure network managed by the DOD that is limited to authorized United States government users.

(1) SIPRNET is a worldwide network capable of providing a secure infrastructure for the exchange of voice, video, data, and imagery, although not all of these capabilities are available to every user, primarily due to equipment configuration and bandwidth restrictions.

(2) Much like the regular internet, SIPRNET is a tool that works in the background and is designed to be transparent to the user while allowing for a secure, reliable method of exchanging information and conducting operations.

(3) The SIPRNET WAN is separated from other networks by a combination of physical, procedural, logistical, and cryptographic measures. All information passes through dedicated, encrypted circuits to ensure integrity.

(4) Direct all requests for SIPRNET installation, de-installation and support to Commandant (CG-65) via the chain-of-command. Refer to Secret Internet Protocol Router Network (SIPRNET) Management Policy, COMDTINST 2070.20 (series) for additional specific SIPRNET guidance.

e. 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.

f. Joint Worldwide Intelligence Communications System (JWICS). JWICS is an enterprise administered WAN link encrypted 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.

g. Other Networks. Operationally specific networks exist to meet the CG's requirement to serve the public interest or satisfy treaty requirements. Examples of these networks include, but are not limited to, the National Distress and Response System (NDRS), Communication Systems Network (CSN) and the Differential Global Positioning System (DGPS).

G. Commercial Satellite Communication (COMSATCOM).

1. General. COMSATCOM includes mobile satellite services (MSS) and fixed satellite services (FSS), and provides a high quality, rapid wireless voice or data communication link to deployed/mobile units. These services supplement terrestrial command, control, and communication, and can improve interoperability with commercial vessels complying with the GMDSS. Commandant (CG-642) is responsible for the management of COMSATCOM equipment.

a. Definition. COMSATCOM includes any satellite communication equipment or capabilities which can be acquired from the public sector.

(1) MSS includes any 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.

(2) FSS includes any COMSATCOM equipment that can be used to communicate only while the transmit/receive equipment is stationary.

b. Equipment and Capabilities. The CG has several enterprise COMSATCOM solutions. This equipment provides classified and unclassified voice and data communication on afloat assets or for deployed/mobile units with a validated requirement.

2. Policy.

a. General. Commandant (CG-642) is the asset manager for CG COMSATCOM requirements approved by Commandant (CG-761). Commandant (CG-642) coordinates with the C4ITSC as necessary to meet approved COMSATCOM requirements.

b. Requirements and Equipment Requests. New requirements or requests for permanent installation of COMSATCOM equipment must be approved by Commandant (CG-761) and Commandant (CG-64) and shall follow the ONS guidelines in Chapter 2 of this Manual.

3. Use of Commercial Satellite Communication (COMSATCOM).

a. General. COMSATCOM charges vary significantly by contract and equipment used. In some cases, unconstrained use of these systems would rapidly deplete available operating budgets. Therefore, usage restrictions must be imposed. Contracts and accounts for COMSATCOM services are centrally managed by the C4ITSC.

b. Policy. Specific system policies are provided through Telecommunications Policy record messages as discussed in Chapter 2.D of this Manual. Current Telecommunications Policy record messages and points of contact are available at: https://collab.uscg.mil/lotus/myquickr/Telecommunications_Information/welcome.

4. Satellite Telephones. Requirements for satellite telephones vary throughout the CG. However, equipment procurement and on-air costs can be excessive with unconstrained use. Close monitoring of satellite telephone usage is required to minimize cost.

a. Satellite phones shall not be used when terrestrial phone service is available.

b. Satellite telephones provide no more security than do clear voice radios or cellular telephones. Only when a security module is employed does the system provide communication security.

c. Area and district commanders may approve the use of satellite phone equipment to augment CGTS operationally.

d. Iridium is a component of the Defense Information Systems Network (DISN) and is the only provider meeting all of DOD requirements for secure handheld MSS. DISN MSS is procured through the DISA. DISN services provided by DISA consist of a monthly flat rate per phone with unlimited use. A majority of CG Iridium phones have service through DISN. Unlimited use of DISN Iridium phones is authorized for official business. Other CG Iridium phones are on a commercial service contract where commercial rates apply. Iridium phones on commercial service plans are designated for contingency operations. They may be used for other operations if only clear (non-secure) communications are required. However, service plan costs shall be considered and morale calls on commercial accounts are not authorized.

(1) The C4ITSC is the sole provisioning agent for EMSS Iridium phones on the DOD contract, including obtaining secure capabilities. The procurement of services from this contract must be approved by area or district commanders and Commandant (CG-65).

(2) DISN Iridium phones can be identified by removing the back cover and inspecting the subscriber identity module (SIM) card. The first two sets of numbers imprinted on the DISN SIM card are: 89881, 69312, or 89881, 79312. Also, DISN MSISDN (phone numbers) begins with the prefix 8816-763. No commercial MSISDN will duplicate this prefix. Commands are authorized to contact the DISA Iridium contractor at 1-877-449-0600 to verify their DISN SIM number and status.

(3) Commands are responsible for verifying phone service type, DISN or commercial, to prevent misuse of Iridium equipment.

(4) Iridium phones are portable electronic devices subject to policies and procedures outlined in U.S. Coast Guard Information Assurance (IA) for Unclassified Information Systems, COMDTINST 5500.13 (series). Iridium phones become classified when connected to the iridium security module (ISM) and the user personal identity number (PIN) has been entered thereby allowing secure communications. The ISM is a cryptographically controlled item (CCI) and shall be stored and shipped according to Sections 520 and 535, of EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3. The user PIN shall be stored in a safe place and is unclassified (FOUO) when not stored with the ISM with which it is associated. Loss of the ISM with or without the phone is a reportable physical incident requiring report per Chapter 9, EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3.

(5) Specific area policies and procedures are available at:

(a) https://cgportal.uscg.mil/delivery/Satellite/TISCOM/Article/TISCOMCOMSATCOMINFO.

(b) Refer to Chapter 4 and Appendix A of this Manual for guidance on the use of encrypted communications.

(c) Use of DISN Iridium phones for morale calls is authorized per Limited Personal Use of Government Office Equipment and Services, COMDTINST 5375.1 (series), at the commanding officer's discretion.

(d) Airtime costs for DISN Iridium phones are centrally funded. However, repair and replacement of existing phones remains unfunded. Units shall follow specific area procedures provided in the link above for repair or acquisition of new or replacement equipment.

(e) Unless permanent shipboard mounts have been installed per an approved TCTO, Iridium phones are to be used with the handset only. Temporary magnetic mount of external antennas is authorized and may be used as deemed necessary by the command.

(6) Communications checks on low usage Iridium phones (used less than twice a month) shall be conducted at least once a month to ensure the equipment is ready for operations. Phones capable of secure communications shall be tested in both clear and encrypted modes.

e. Satellite phone use on aircraft must be approved by Commandant (CG-41) and requests must also complete the Aircraft Configuration Control Board (ACCB) process. Refer to the Coast Guard Air Operations Manual, COMDTINST M3710.1 (series).

H. Military Satellite Communication (MILSATCOM).

1. General. MILSATCOM is the DOD satellite constellation that provides near global operational communications (including Polar Regions) for military aircraft, ships, submarines and ground stations to meet their requirement for rapid, reliable, secure and hardened communications throughout the DOD.

a. The CG requires access to MILSATCOM for interoperability with the USN and DOD in time of war as per U.S.C. Title 14 § 3 and also to meet CG, DHS and interagency missions in peacetime. U.S Navy – U.S. Coast Guard Communications Policy, OPNAVINST 2000.20D is an agreement that outlines support the USN agrees to provide to the CG to meet MILSATCOM interoperability requirements. Our allies and other government agencies also use MILSATCOM.

b. Military satellites were originally built for three specific user groups. The Defense Satellite Communications System (DISCUS) serves the wideband users, the Fleet Satellite Communication System (FLTSAT) serves the mobile/tactical (narrowband) users and the Military Strategic & Tactical Relay Satellite System (MILSTAR) serves the protected users. As the need for channels increased, the DOD responded by leasing the Leased Satellite (LEASAT) satellites and deploying the UHF Follow on (UFO) satellites. Both provided additional narrow/wideband channels in response to the increased demand within those user groups. MILSAT channels are also hosted on allied satellites such as SKYNET (UK satellite system).

c. The CG uses MILSATCOM in the extremely high frequency (EHF) and UHF bands. United States Northern Command (NORTHCOM) located in Colorado Springs, Colorado, is the DOD MILSATCOM sponsor for the CG. NORTHCOM validates all CG MILSATCOM requirements for UHF and EHF access. The overall DOD satellite communications manager is Commander, United States Strategic Command (USSTRATCOM). Subordinate to USSTRATCOM is the combatant commands (COCOM). The COCOM manages all SATCOM resources within their specific AOR, similar to the functions of CG Area offices.

2. Definition. MILSATCOM is defined as the constellation of satellites used by the DOD for rapid, reliable, secure and hardened communications in the UHF, super high frequency (SHF) and EHF bands. This also includes the polar satellites known as Satellite Data System (SDS) and Package D. Both provide UHF channel access and can be used for EHF but only in the low data rate mode.

a. Demand Assigned Multiple Access (DAMA). DAMA was developed to multiplex several baseband systems or users onto one 25 kHz (kilohertz) channel. This significantly increases the amount of available channels. Prior to DAMA, each UHF circuit required a single channel. 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.

b. Non-Demand Assigned 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 (e.g., CG Tactical Information Network (TIN)).

c. Legacy. Legacy MILSATCOM refers to all equipment that is not integrated waveform (IW) capable (e.g., LST-5D, TD-1271).

d. Multi-band Radio. Multi-band radio refers to the newer generation of radios that can operate in more than one band.

e. Mobile User Objective System (MUOS). MUOS will replace the existing UFO system prior to it reaching its end-of-life. Once in service, MUOS will

be capable of serving additional users with greater mobility, capacity, and quality of service than the former UFO system was capable of accommodating. MUOS will be a limited protected narrowband (64 kbps and below) satellite communication (SATCOM) system that will support a worldwide, multi-service population of mobile and fixed-site terminal users. The MUOS legacy payload will continue to provide interoperability with the legacy terminals while the MUOS constellation achieves full on-orbit capability.

f. Integrated Waveform (IW). IW is a new UHF SATCOM waveform that requires software or hardware upgrades to be installed on UHF SATCOM terminals and will be a standalone channel control system at four operational sites. This waveform can more than double the current UHF SATCOM accesses available using legacy DAMA. It will provide increased capability to mitigate any potential MUOS schedule delays as well as anticipated UHF SATCOM constellation failures.

g. Joint Tactical Radio system (JTRS). JTRS is a new generation DOD developed multiband radio systems intended to replace the legacy MILSATCOM terminals and to be used with the new MUOS satellites. In addition to these radio systems, various vendors are producing JTRS capable radios, of which, some are currently available (e.g., PRC-117G). JTRS will provide MUOS waveform to access the on demand 2.4 to 64 kbps beams for voice and data services.

3. Equipment and Capabilities. The C4ITSC is responsible for all MILSATCOM equipment throughout the CG and uses Space and Naval Warfare Systems (SPAWAR) Command to maintain these systems. For a complete overview of MILSATCOM equipment, refer to the following site: https://cgportal.uscg.mil/delivery/Satellite/C2CEN/MILSATCOM.

4. Use of Military Satellite Communication (MILSATCOM). CG specific MILSATCOM circuits can be found in Chapter 7 of this Manual. The following is a listing of DOD circuits used by the CG, although not all inclusive:

   a. Satellite High Command (SATHICOM) (USN tactical voice);

   b. Joint Interagency Task Force (JIATF) air (JIAFT South tactical voice);

   c. JIATF surface (JIATF South tactical voice);

   d. Common User Digital Information Exchange System (CUDIXS) - used for tactical Top Secret and below messaging and operator-to-operator communications with the USN record message servicing facility;.

   e. Fleet Broadcast (USN record message system capable of Top Secret but currently used for Secret and below general record message traffic);

f. TIN – used by both areas to pass tactical data such as common operational picture (COP) via a 5 kHz MILSATCOM channel; and

g. Imaging and Communications Environment (ICE) – used by Maritime Intelligence Fusion Centers (MIFC) and certain aviation assets to pass imagery data. ICE also uses a 5 kHz MILSATCOM channel.

h. Columbian Navy (COLNAV) - JIATF Columbian Navy Circuit.

5. Policy. Commandant (CG-761) is the sponsor for all enterprise MILSATCOM requirements. Commandant (CG-64) works with the C4ITSC to provide solutions to meet validated MILSATCOM requirements.

a. Commandant (CG-761) reviews and validates all MILSATCOM requirements. Once requirements are validate they are submitted to NORTHCOM for review.

b. The review process involves entering the validated CG requirement into the DOD satellite database (SDB) and submitting the new requirement to NORTHCOM who in turn starts the DOD validation process. The requirement receives a technical review from the SDB administrator. Upon completion of this review, it is submitted to the Joint Satellite Panel (JSP) for review. The JSP meets monthly to review all newly submitted SATCOM requirements. If approved by the JSP, the SDB is updated to reflect a validated requirement for MILSATCOM use, and the requirement owner/user will be allowed to access MILSATCOM satellites.

c. Approved requirements require an annual revalidation. This ensures CG units can access authorized channels as needed to meet mission needs.

d. Access to EHF satellites is authorized on a per mission basis. The satellite access request is sent to NORTHCOM. NORTHCOM approves requests and validates requirements through entry in the SDB. NORTHCOM works with the Global SATCOM Support Center (GSSC) to provide the service for the required dates. Approved EHF satellite access is valid only for the dates specified in the satellite access authorization (normally the duration of the patrol).

e. Specific policies for access and satellite access request submissions are outlined in CJCSI 6250.1D, Satellite Communications.

f. CG units requiring MILSATCOM access must contact the servicing facility to ensure all local procedures are followed when submitting access requests. The CAMS promulgate their MILSATCOM access procedures through LANTCOMMSYS/PACCOMSYS series record messages.

g. A terminal base address (TBA) is required for each MILSATCOM circuit that accesses a DAMA channel. This process must be completed or servicing MILSATCOM facilities cannot provide access. TBA requests can take up to

30 days for approval and issuance. All TBA requests must be submitted to the C4ITSC.

6. Security. CG MILSATCOM users shall ensure they use the appropriate cryptographic KEYMAT for the MILSATCOM circuits used and that the equipment is safeguarded per the guidelines of Chapter 4 of this Manual.

7. New Requests for Military Satellite Communication (MILSATCOM) capability.

   a. New requests for MILSATCOM equipment shall be documented following the ONS guidelines in Chapter 2.B of this Manual.

   b. If the compilation of this information is classified, requesting units shall ensure appropriate security measures are used to prevent disclosure of classified information. If in doubt, consult district or areas security managers.

   c. Commandant (CG-761) review and approval only validates the need for the MILSATCOM capability and does not constitute approval to purchase MILSATCOM systems.

   d. Commandant (CG-64) will approve MILSATCOM equipment acquisitions provided Commandant (CG-761) has approved the requirement and adequate resources are in place to purchase and support the equipment.

8. Unauthorized Installations. MILSATCOM systems procured or installed outside of approved requirements are not authorized and subject to removal.

   a. Units shall notify Commandant (CG-64) and their operational control (OPCON) to report any MILSATCOM systems that may not be authorized to ensure all assets are reflected in the unit's allowance list.

   b. This allowance list, in conjunction with a completed OPNAV 4790, permits the proper tracking of each unit's configuration in the Fleet Logistics System (FLS).

9. Time Compliance Technical Order (TCTO). The addition of MILSATCOM systems constitutes a change to the unit's communication configuration, so all units shall ensure a TCTO is submitted and approved prior to any system installation.

10. Cryptographically Controlled Item (CCI). Most MILSATCOM radios are CCI and shall be kept under positive control at all times, to include being tracked by the unit EKMS manager. All new MILSATCOM radio purchases shall be coordinated with the unit EKMS manager to ensure proper transfer and storage. In addition, the unit EKMS manager shall advise the C4ITSC (BOD-IAB), via the EKMS immediate-superior-in-command (ISIC) of all new MILSATCOM radio procurements.

I. Procurement of Telephone, Network or other Commercial Communication Services.

1. General. As noted in Chapter 5 section C.1, CG DARs are the only authorized agents allowed to place orders for telecommunication circuits and services (excluding cellular wireless) from approved sources and shall use the most current policy and practices promulgated by the C4ITSC.

2. Unavailable Services. For services not available under the current federal contract, BSUs/ESUs shall work with the C4ITSC to contract intra-area data circuits through Defense Information Technology Contracting Organization (DITCO) per DISA Circular 310 130 1.

3. Requests/Modifications. Requests or modifications for DISN, DOD, or other department or agency services shall be submitted to the C4ITSC as requests for service (RFS).

4. General Services Administration (GSA). GSA must approve administrative services per applicable federal regulations. DISN circuits and services are operational, not administrative, in nature.

5. Requests for Enterprise Data Network Services. Area and district commanders, unit commanding officers, and directorates and special staff divisions at Headquarters shall submit requests for enterprise data network services to the C4IT SC via their chain-of-command. All requests shall be made via official CG memorandum. The use of CG E-mail is not sufficient to satisfy contractual and fiscal commitments. All requests shall include:

   a. Type of access desired (CGOne dedicated, CGOne frame relay, DHS OneNet, NIPRNET, SIPRNET, JWICS etc.);

   b. Desired installation date (most provisioning activities take 90-120 days on average);

   c. Type of terminal and protocol (e.g., government furnished equipment (GFE) router);

   d. Location: Street address (no post office (P.O.) boxes), demark location (room name/number), service delivery point, demark manager (if building is leased or on a DOD facility);

   e. Unit POC (include telephone number, FAX number, and E-mail address);

   f. Area code and prefix (NPA/NXX) for existing service at the address specified in item (4) above;

   g. Any known telephone numbers or data circuit numbers at the address specified in item (4) above;

   h. Servicing ESU/ESD POC; and

i. Funding for moves and changes to the networks include installation (non-recurring changes (NRC)) and monthly maintenance costs (monthly recurring charges (MRC)).

Upon receipt of the memorandum, the C4ITSC provides a quote for the service requested, including anticipated NRC and MRC for the remainder of the current fiscal year, in addition to the units commitment for MRC charges for follow-on years. Anticipate collection of annual fees (MRC) at the beginning of every follow-on fiscal year once the budget is approved.

6. Coast Guard (CG) Telecommunication Certification Office (TCO). Designated TCOs shall comply with all DISA/DITCO policies and procedures for requesting telecommunication services or facilities.

   a. A TCO code designates the command responsible for certifying and funding a circuit requirement.

   b. The TCO codes are used as the first two characters of all order numbers issued to DISA/DITCO.

   c. The applicable codes are listed in Exhibit 5-1.

Exhibit 5-1
TCO Command Codes

Commanding Officer, CG TISCOM	CC

7. Program Designator Codes (PDC). Orders for new service and requests for changes in service shall include a PDC. This is a six character code used by DISA/DITCO for billing purposes.

   a. Derive the first four characters of the PDC from Exhibit 5-2.

Exhibit 5-2
Program Designator Codes (Characters 1-4)

Commanding Officer, CG TISCOM	W2GA	W2GB	W2GC	W2GD
	W2GH	W2GJ	W2GK	W2GL
	W2GM	W2GN	W2GQ	W2GR
	W2GS			

   b. Derive the fifth character of the PDC from Exhibit 5-3. This character shall be assigned by the cognizant TCO to identify the program that the circuit supports. Use character (Q), Communication Services, for multi-use circuits.

Exhibit 5-3
Program Designator Codes (Character 5)

Character	Program
A	Search and Rescue
B	Short Range Aids to Navigation
C	Radio Navigation Aids
D	Commercial Vessel Safety
E	Port Safety and Security
F	Marine Environmental Protection
G	Polar Ice Operations
H	Domestic Ice Operations
I	Marine Science Activities
J	Reserve Forces
K	Military Operation/Preparedness
L	Personnel (including training)
M	Engineering
N	Financial Management, Personnel Supply
O	Research, Development, Test, and Evaluation
P	Law Enforcement, Intelligence, and Security
Q	Communication Services
R	Bridge Administration
S	Recreational Boating Safety
T	Medical Support
U	Legal Support
V	Safety and Health
W	Civil Rights

c. Derive the sixth character of the PDC from Exhibit 5-4 to indicate the circuit type and purpose.

Exhibit 5-4
Program Designator Codes (Character 6)

Character	Circuit Usage and Type
A	Frame Relay
B	Asynchronous Transfer Mode (ATM)
C	DISA/SIPRNET
D	DISA/NIPRNET
E	VHF-FM Guard 156.8 (MHz)
F	VHF-FM Select
G	MF-AM Guard 2182 kHz
H	MF-AM Select
I	DISA Subscription Services
J	TBD
K	Equipment Lease
L	TBD
M	Network Operation Center Services (NOC)
N	Network Operation Center Services (NOC)
O	TBD
P	TBD
Q	Equipment Purchases (Modem/Cables/VTC Equipment)
R	TBD
S	EMSS/Iridium Equipment and Services
T	HFCG Broadcast Network 4.8kbps; also T3 Data circuits
U	Data Circuit, 9,600 BPS
V	Data Circuit, 19, 200 BPS
W	Data Circuit, 56, 000 BPS
X	Data Circuit, 1,544 MBPS
Y	FX Trunk
Z	Tie Lines (PBX to PBX)
1	Voice (Other)
2	Data (Other)
3	TBD
4	Fleet55 PATFORSWA
5	Fleet77
6	INMARSAT-A (Obsolete in the CG)
7	INMARSAT-C
8	INMARSAT-M
9	INMARSAT-B

8. National Communications System (NCS). The NCS was established to provide better communications support to critical government functions during emergencies. The NCS mandate includes linking, improving and extending the communications facilities and components of various federal agencies, focusing

on interconnectivity, survivability and National Security and Emergency Preparedness (NSEP) to support crisis and disasters.

a. The following programs are sponsored by the NCS:

(1) NSEP telecommunication services are those services critical to the maintenance of a state of readiness or the response to and management of any event or crisis which causes or could cause harm to the population, damage to property, or threaten the security of the United States; and

(2) The Telecommunication Service Priority (TSP) program provides priority provisioning and restoration of telecommunication services. TSP Program Management is delegated to Commandant (CG-6) the C4ITSC is the lead SSA. Commandant (CG-6) further delegates ordering functions to the C4ITSC. Management and ordering functions shall be as per the most current policy and practices promulgated by NCS and the C4ITSC.

b. All commands designated TCO authority shall maintain the NCS database for circuits under their cognizance as per NCS Bulletin 55-2.

CHAPTER 6 TELECOMMUNICATIONS ADMINISTRATION: RECORDINGS, INTERFERENCE AND VIOLATION REPORTS, RECORDS, UNIT LOGS, AND INSPECTIONS

A. Purpose. To set forth policy and provide guidance for the preparation, submission, retention and disposal of communication recordings, reports, records, and logs.

B. Use of Recording or Monitoring Equipment.

1. SECDHS policy forbids department personnel from engaging in clandestine, surreptitious, or other covert use of telephone recording, listening, or monitoring equipment, or from aiding or acquiescing in the use of such equipment, in the conduct of their official duties. More specific requirements for individual units are detailed in subsequent applicable Chapters.

2. Digital Voice Logger (DVL) and R21 System recording equipment is required at all CG units (less stations and boats under 65 feet) to record telephone and/or radio communications where such communications may relate to the safety of life and property, including but not limited to air safety, maritime safety and SAR, and CG tactical communication operations. The CG does not require beep tones or prior consent for the recording of these conversations.

3. Equipment installed on telephone lines only to provide a recorded announcement or voice mail service is considered office labor saving rather than communication or electronics equipment and does not require approval.

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

C. Communication Reports. Except for those reports specifically discussed in this Chapter, communication reports shall be submitted as per Chapter 7 of the Directives, Publications, and Reports Index (DPRI), COMDTNOTE 5600. Guidance for COMSEC reports, logs, and files can be found in Annex S of EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3. The COMTAC Publication Policy and Procedures Manual, COMDTINST M2600.1 (series) shall be consulted for allied communication reports and files. Area commanders requiring further reporting shall provide specific guidance in their Annex K to Area OPLAN.

1. Joint Spectrum Interference Report (JSIR) – Report of Radio Interference. Communication operators shall report all cases of harmful interference regardless of type, frequency, and source. A definition of harmful interferences is described in Chapter 4 of Spectrum Management Policy and Procedures, COMDTINST M2400.1 (series). The JSIR message format is contained in Appendix D of Spectrum Management Policy and Procedures, COMDTINST M2400.1 (series).

   a. When harmful interference to spectrum dependent systems is experienced, a JSIR shall be submitted. A single report summarizing a case of harmful

interference over an extended period of time (not to exceed one month) may be submitted after the initial report.

b. Units experiencing radio interference shall use all available resources such as the local FCC office, military departments, C4ITSC and district spectrum managers, and/or ESU to determine the source of the interference.

c. Area commanders shall ensure a point of contact resource list is contained in their Annex K to Area OPLAN.

2. Report of Violation of the Radio Regulations or Communications Instructions, Form CG-2861A. Radio violation reports shall be submitted as per Chapter 4 of the Spectrum Management Policy and Procedures, COMDTINST M2400.1 (series) for violation of national or international radio regulations.

a. For violations committed by CG units, submit the original copy of the Report of Violation of the Radio Regulations or Communications Instructions, Form CG-2861A, to the violating unit, a copy to the violating unit's area and district commander, a copy to the reporting unit's district commander, and retain a file copy.

b. For other violations refer to Chapter 4 of Spectrum Management Policy and Procedures, COMDTINST M2400.1 (series), or consult your C4ITSC or district spectrum manager.

c. A sample copy of the Report of Violation of the Radio Regulations or Communications Instructions, Form CG-2861A, is located in Appendix D of Spectrum Management Policy and Procedures, COMDTINST M2400.1 (series).

D. Communication Records. Communication records are defined as any type of media format used to record official information that has been transmitted, received or written down.

1. Search and Rescue (SAR) Communication Records. CG units shall maintain communications documentation for situations in which resources coordinate or render assistance, regardless of position or location of the incident (e.g., medical communications (MEDICO)). The intent is to ensure CG resource activity is properly documented to support analysis of SAR operating needs, management and budgetary decisions.

a. SAR communication case documentation may include, but is not limited to, the following examples:

(1) Logs and diaries. Logs and diaries may be either electronic or paper documentation created and collected from start to finish of an active case;

(2) SAR forms/check sheets. SAR forms and check sheets (e.g., initial SAR check sheet) serve many purposes (e.g., documenting information from the

distressed craft, facilitating communication between responding units, briefing crews, search planning);

(3) SITREP's, UMIB's, etc; and

(4) Audio/video files.

NOTE: If recorded radio transmissions, telephone calls and video recordings must be retained (see retention requirements in section F of this Chapter), then the audio and video files shall include sufficient information to completely re-create the case, so far as possible, and to show the rationale for all decisions made.

b. The AUX shall follow the same communications record keeping requirements as set forth in section C, D, and E of this Chapter or as modified by the area commander.

c. Units equipped with R21 shall include all line of bearing, digital selective calling (DSC) and caller detail information in SAR case documentation.

d. Further guidance, including requirements for Marine Information for Safety and Law Enforcement (MISLE) entries, can be found in 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).

2. Additional Operational Records. Area and district commanders may require additional reports and copies of various operational communication records originated or received, and shall ensure relevant guidance is provided in their Annex K to Area OPLAN or Operational Tasking (OPTASK) COMMS. Examples include SIPRNET CHAT (SIPRCHAT) or other similarly purposed formally established operational chat circuits.

E. Daily Communication Logs.

1. General. Daily communication logs serve as official documents to record communications and related events concerning the administration of the command and also to provide a record that may be the subject of investigation or legal action.

2. The two types of communications logs maintained are an abbreviated log and a complete log:

a. Complete log. A paper, electronic or recorded log that contains all communication data a unit sends or receives. Units with recording equipment are not required to maintain a complete log (paper/electronic) unless the recording equipment fails.

b. Abbreviated log. A manually maintained paper or electronic log that uses abbreviations and known acronyms for all communication data sent or received that pertains to the unit. Verbatim entries are not required or encouraged. Standard acronyms, abbreviations, designators, symbols, and signals appearing in official publications (ACPs, NTPs, and ITU publications) shall be used. An abbreviated log provides the command a synopsis of communications and events that occurred throughout the day.

3. Recorder Casualties. In the event of a recorder casualty, the unit shall maintain a complete log to capture all transmissions pertaining to that unit. The accuracy and completeness of this log is extremely important as it serves as the only unit communication record available until such time as the recorder is repaired. Units shall hold quarterly training on maintaining a complete manual log in the event of a recorder casualty.

4. Communication Log Requirements.

a. Daily communication logs are required for all radio equipped units (including CG AUX) and deployable communications assets (e.g., Mobile Command Vehicle (MCV), enhanced Mobile Incident Command Post (eMICP), Transportable Communications Central (TCC)) with the following exceptions:

(1) Vessels over 65 feet (e.g., buoy tenders, patrol boat) and not equipped with a recorder or a dedicated communication watch are exempt from log requirements. The bridge smooth log may be used for abbreviated communication entries if desired;

(2) Vessels under 65 feet in length;

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

(4) Unit vehicles equipped with very high frequency-frequency modulated (VHF-FM) or personnel deployed with handheld communications equipment; and

(5) Shore units that maintain some type of communication guard but are not equipped with recorders;

b. Communication logs may be paper, electronic and/or recorded on a DVL or within the R21 system.

c. All communication logs (less recorded logs) shall be reviewed for completeness and accuracy by a supervisor prior to submission to the commanding officer.

d. Recorder-equipped units shall maintain an abbreviated log (manual or electronic) along with the recording.

e. Logging of all distress, urgency, or safety signals and related communication made or intercepted on any frequency or circuit is required, regardless of the type of log maintained and as appropriate for the type of log maintained. Required information in abbreviated log entries for distress, MEDICO, and urgent signals shall contain the originator, frequency, time and a brief synopsis of what occurred. The recorded log shall be referred to as necessary for more information. These events shall be logged until it is apparent they do not relate to the geographic area or that the unit will not play a part in the actual assistance.

5. Content. The following information, at a minimum, shall be identified in communication logs:

   a. Unit (may be identified using record message Plain Language Address (PLA));

   b. Call sign;

   c. Date and time (Coordinated Universal Time (UTC), identified as Z);

   d. Frequency/channel;

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

   f. Communications equipment status.

6. Manual Logs. Manual logs are handwritten, typewritten, or kept on a CG computer or other information processing equipment such as electronic Radio Logs (RADLOGS) software. If not typewritten, all entries shall be handwritten in blue or black ink.

   a. Log entries shall not be erased. All changes to the log are made by drawing a single line in ink or typing slant signs through the original statement, indicating the changed version adjacent to the original entry. All changes to the communication log must be initialed in ink. When an electronic (computer or information processing equipment) communication log is used, change procedures identified above are waived. Log corrections to abbreviated logs are authorized after signature to maintain consistency with recorded logs; however, no changes to a complete manual log or its associated electronic file shall be made once signed by the operator. This would only apply if the manual abbreviated log is taking the place of the recorded log due to a casualty.

   b. 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.

c. Examples of communications logs can be obtained from the Operations Specialist (OS) "A" school staff.

7. Electronic Communication Logging Software. RADLOGS provides a database-driven operational logging system for operations personnel. RADLOGS is currently operating at each CAMS and COMMSTA Kodiak, with a single component of RADLOGS called Electronic Status Board (ESB) at Air Station Kodiak. Units equipped with RADLOGS shall follow the log keeping policy of this Chapter when applicable (e.g., signatures, retention).

   a. In addition to required logging information, RADLOGS has features engineered into the software to transfer communication guards from watch station to watch station within the CAMS or to the opposite CAMS.

   b. The RADLOGS program meets the requirement for a backup abbreviated log at units with recorders and the RADLOGS software.

8. Recorded Logs. Recorded logs (e.g., DVL, R21 system recorded files) are logs recorded on electronic media. Recorded logs relieve the operator of complete logging responsibility. Units with recorded logging capability shall maintain abbreviated logs as a backup in case the recorder fails. Attach a label to each recorded log disk that indicates:

   a. Unit name and call sign;

   b. Date and period recorded in UTC; and

   c. Frequencies and/or phone lines recorded. If a large number of frequencies and/or phone lines are recorded, a detailed listing is not required on the label if the information is available from other sources (e.g., supervisor's log, technical control log).

F. Retention of Files, Reports, Records, and Logs.

1. Search and Rescue (SAR) Case Files. SAR case files shall be retained as per 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).

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 United States, a case under litigation, or an incomplete investigation, shall 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 an 18 month period

after the incident). For this reason, if any personal injury, death and/or property damage occurs while the CG is rendering assistance to the public, the unit(s) involved shall immediately consult Chapter 2 of the Coast Guard Claims and Litigation Manual, COMDTINST M5890.9 (series) and their servicing legal office to determine if the SAR/MEDICO/Incident audio files need to be retained beyond 30 days. The commanding officer/officer-in-charge of the case, after consulting with legal staff if it is deemed necessary, shall make the determination as to whether the audio files should be retained more than 30 days.

b. If retention is required, the involved unit(s) shall ensure all files pertaining to the case or incident are retained for a period of 2 years or until the claim is resolved, whichever occurs first.

3. Audio Files. Audio files consist of radio transmissions and telephone calls and, except as noted in sections F.1 and F.2 of this Chapter, shall be retained for 30 days. On the R21 system, excepted as noted in sections F.1 and F.2 of this chapter, all audio files are stored on the hard drive for at least 30 days. Audio recordings are meant to be used as an operational tool. However, there are circumstances where it may be desirable to retain audio files or copied portions of audio files. This includes incidents of national significant, potential litigation, and liability cases.

4. Joint Spectrum Interference Report (JSIR) – Report of Radio Interference. JSIRs are reported as record messages and shall be retained per record message retention requirements (See Chapter 10 of this Manual).

5. Report of Violation of Radio Regulations or Communication Instructions, Form CG-2861A. All violation reports shall be kept on file for a period of 3 years from the date of the incident.

6. Visitor Register. Visitor Registers are any register or log used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers. Retain for 2 years after final entry or 2 years after date of document, as appropriate.

7. Record Messages. See Chapter 10 of this Manual.

8. Communication Logs. Cutters retain for 90 days, shore units retain for 6 months.

9. Telecommunications General File (SSIC 2000-2999). Includes plans, reports, and other records pertaining to equipment requests, telephone service, and like matters. Retain for 3 years.

10. Telecommunications Operational Files (SSIC 2000-2999). Includes record message registers, logs, performance reports, daily load reports, and related and similar records. Retain for 6 months.

11. Telephone Use (Call Detail) Records. 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.

12. Incidents of National Significance. Permanent retention. Communication records qualifying for permanent retention shall be maintained at the unit that prosecuted the case or incident for 3 years and then transferred to a Federal Records Center (FRC) as outlined in section I, Chapter 2 of Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). The following criteria shall be applied to determine if communication records qualify:

    a. Incidents or cases identified as having historical significance due to the scope or nature of the case, or cases involving prominent persons. Examples include:

        (1) Cases of prominent persons of national or regional context,

        (2) Cases receiving national or regional media attention,

        (3) Cases used in Congressional or other oversight investigations,

        (4) Cases involving a great number of persons seeking rescue,

        (5) Incidents of national significance such as a terrorist attack or natural disaster, and

        (6) Cases representing substantive change in agency policy and procedures;

    b. Consult with the records coordinator for further assistance; and

    c. Administrative and non-essential communication records (paper, electronic or recorded) shall be retained for 90 days.

G. Disposal of Files, Reports, Records, and Logs. All communication files, reports, records, and logs not requiring transfer to the FRC and meeting specified retention requirements may be destroyed (i.e. burning, shredding) without report, except as directed by appropriate authority. For guidance on extraordinary events, review Information and Life Cycle Management Manual, COMDTINST M5212.12 (series).

H. Telecommunication Inspections. Area, district and sector commanders shall inspect their subordinate radio communication equipped units biennially. Checklists for these inspections shall be included in their Annex K to Area OPLAN and District Supplements.

1. Purpose. The primary purpose of this inspection is to evaluate the unit's ability to fulfill its telecommunication responsibilities from both a materiel and a personnel training resource perspective.

a. Routine paperwork compliance with the various publications and directives governing all telecommunication procedures and administration shall be given secondary status to this primary purpose.

b. Exercise all telecommunications systems and contingency procedures during the visit whenever possible.

2. Pre-Brief/Post-Brief. Prior to and after completion of the telecommunication inspection, a pre-brief and post-brief detailing the visit is recommended. The commanding officer or appointed representative from the command being visited should be present during both briefs.

3. Inspection Reports. The inspecting command shall forward a written report of the visit findings.

a. Note all deficiencies and inoperative systems.

b. Include specific comments as to what follow-up action is recommended and the office in the chain-of-command tasked with the follow-up action.

c. Units shall have 90 days to complete and report corrective/follow-up action.

4. Tracking. Areas (LANT-6/PAC-6) and districts (dt) shall be responsible for tracking inspection schedules and the report and response timeframes.

CHAPTER 7 COAST GUARD (CG) SHORE TELECOMMUNICATION FACILITIES AND FUNCTIONS

A. General. CGTS facilities include the EMF, CAMS, mobile and deployable systems, CCs, Air Stations (AIRSTA) and Vessel Traffic Service (VTS). The following sections describe and detail policies pertaining to the operation and maintenance of these units. Additional sections describe units providing support or products for communication operations.

B. Command, Control, Communications, Computers and Information Technology Service Center (C4ITSC). C4ITSC provides full life-cycle support for CG C4IT applications, systems and infrastructure enabling CG personnel to have the information they need to perform their jobs effectively. C4ITSC oversees the operation of the three C4IT centers of excellence: OSC, TISCOM and C3CEN.

1. Command, Control, Communications, Computers and Information Technology (C4IT) - Operations System Center (OSC). OSC provides full life cycle support for operationally-focused CG enterprise-wide information systems. OSC develops, fields, maintains and provides user support to improve CG mission performance through the innovative application of technology.

2. Command, Control, Communications, Computers and Information Technology (C4IT) - Telecommunication and Information Systems Command (TISCOM). TISCOM provides full life-cycle support for enterprise information systems infrastructure. TISCOM develops, fields, maintains and provides user support to improve CG mission performance through the innovative application of technology.

3. Command, Control, Communications, Computers and Information Technology (C4IT) - Coast Command ,Control and Communications Engineering Center (C3CEN). C3CEN develops, builds, fields and supports advanced electronic command, control, communication and navigation systems. C3CEN facilitates evolutionary engineering that focuses on the rapid deployment of essential functionality followed by planned improvements based on enhanced or refined requirements. In addition to providing maintenance and troubleshooting assistance on its assigned systems that is beyond the scope or capability of intermediate level support, C3CEN provides a point of contact for technical liaison and information.

C. Coast Guard (CG) Navigation Center (NAVCEN). NAVCEN is the primary public source of information for CGTS public services. NAVCEN's Maritime Information Operations Center (MIOC) watch provides a 24x7 monitoring of DGPS, Long Range Identification and Tracking (LRIT), National Automated Identification System (NAIS) Increments 1 & 2, and the Navigation Information Service (NIS). NAVCEN provides the general public with maritime telecommunications information and services on its web site: www.navcen.uscg.gov.

D. Communication Area Master Station (CAMS) and Communication Station (COMMSTA).

1. Organization. Each area commander is supported by a CAMS. Communication Area Master Station Atlantic (CAMSLANT) and Communication Area Master Station Pacific (CAMSPAC) are under the operational and administrative control of LANTAREA (LANT-6) and PACAREA (PAC-6). The CAMS provide rapid, reliable, and secure communications for CG operational commanders, other government agencies and the maritime public.

2. Purpose. The commanding officer of the CAMS is responsible for the organization, operation, and supervision of the CAMS. The CAMS provide voice, data and record message delivery services for all CG cutters, aircraft, and shore units located within their geographic areas. Additionally, CAMS provide other military organizations, government agencies, and the civilian sector a capable means of communication both secure and non-secure on a regular basis or during a crisis or emergency situations

3. Communication Station (COMMSTA). COMMSTA's are subordinate units under the operational and administrative control of the CAMS. With the exception of COMMSTA Kodiak, Alaska, COMMSTA operations are remotely controlled by their CAMS and no longer stand 'live' operations watches. Each COMMSTA is staffed with technicians to maintain and supervise the operation of transmitters, receivers, antennas, and associated equipment. Exhibit 7-1 lists CAMS facilities and their associated call signs under the CAMS responsible for broadcast operations:

Exhibit 7-1
Facilities and Associated Call Signs

CAMSLANT (NMN)	CAMSPAC (NMC)
COMMSTA Boston (NMF)	COMMSTA Kodiak (NOJ)
COMMSTA Miami (NMA)	COMMSTA Honolulu (NMO)
COMMSTA New Orleans (NMG)	CG Guam (NRV)

4. Communication Area Master Station (CAMS) Services. Each CAMS has specific telecommunication responsibilities vital to the CGTS. CG telecommunication services provided by the CAMS for CG units, government agencies, or the maritime public are as follows:

a. Area-Wide Communication Center (AWC). The AWC provides record messaging services throughout the CG and DHS. Additional details on CAMS record messaging services are contained in Chapter 10 of this Manual.

Note: CAMSLANT manages all CG record messaging collective addresses and is responsible for the maintenance of CG general record message files.

See Chapter 10 of this Manual for additional messaging duties and responsibilities of CAMSLANT.

b. High Frequency (HF) Command and Control Networks. Serve as primary Net Control Station (NECOS) within their geographical area for HF Secure Voice Network (SVN) services to accommodate sensitive or classified conversations on CG HF circuits.

c. High Frequency (HF) Automatic Link Establishment (ALE) Networks. The CAMS and COMMSTA Kodiak operate HF ALE command and control networks providing voice services to CG vessels and aircraft. ALE capable HF systems keep track of signal quality to/from each network member, ultimately improving HF communication. ALE provides a Link Quality Assessment which determines the optimum transmission frequency at any given time. ALE also removes some of the HF operational variables and complexities for the user.

(1) Cellular over the Horizon Enforcement Network (COTHEN). CBP operates and maintains COTHEN from the NLECC in Orlando, Florida. A CAMSLANT detachment is assigned to the NLECC.

(2) Geo-Spatial over the Horizon ALE Matrix (GOTHAM). COMMSTA Kodiak operates GOTHAM as a CG ALE network. GOTHAM provides both clear and secure communication within CG District 17 AOR.

(3) HF ALE Procedures. Specific guidance and procedures for access to HF ALE services can be found at: http://cgweb.rss.uscg.mil/communicationsportal/content/HQ_GMF/hf_ale.aspx.

d. Coast Guard (CG) Marine Information Broadcast (MIB). Each CAMS and COMMSTA Kodiak shall broadcast weather and hydrographic information, storm warnings, and notice to mariners. Specific responsibilities and marine information broadcast schedules shall be prescribed in their Annex K to Area OPLAN and unit SOP's. Schedules are made available to the general public at on the NAVCEN's website. The following broadcast modes are conducted by the CAMS and COMMSTA Kodiak:

(1) HF radio FAX, including International Ice Patrol FAX;

(2) HF voice, medium frequency (MF) voice;

(3) Navigational Telex (NAVTEX); and

(4) HF Simplex Teletype Over Radio (SITOR)

e. Aircraft High Frequency (HF) Flight Following Services. Provide aircraft safety of flight services using CG secure air-to-ground (SAG) and CG non-secure-air-to ground frequencies and CBP's COTHEN.

f. Military Satellite Communication (MILSATCOM) Networks. The CAMS use separate military satellites to provide coverage in their AORs.

(1) Communication Area Master Station Pacific (CAMSPAC).

(a) Homeland Security Net (HLS-Net). (DAMA and Non-DAMA merged tactical voice net. Net control station (NECOS)).

(b) TIN. Data only (NECOS).

(c) Circuits under development:

[1] IW Voice (CG transition circuit to IW).

[2] IW Data. Future tactical data circuit.

(2) Communication Area Master Station Atlantic (CAMSLANT).

(a) HLS Net. (DAMA and Non-DAMA tactical voice net. (NECOS)).

(b) TIN. Data only (NECOS).

(c) Circuit under development: IW Voice (CG transition circuit to IW).

g. Global Maritime Distress and Safety System (GMDSS). MF and HF DSC and GMDSS voice frequency guard. DSC and other GMDSS networks are used for ships to alert coastal stations of distress or other safety-related conditions. Refer to Chapter 11 of this Manual for DSC and GMDSS operations and policy.

h. Communications Assist Team (CAT).

(1) CAT visits provide unit specific training to fleet communicators. A CAT visit is not a communication inspection but rather an assessment of the unit's communications operations. CAT visits have proven very beneficial prior to Command Assessment of Readiness and Training (CART) in preparation for Tailored Annual Cutter Training (TACT)/Tailored Ships Training Availability (TSTA) and are provided at no cost to the units.

(2) For detailed information regarding these services contact the servicing CAMS or refer to LANTCOMMSYS/PACCOMMSYS series record messages.

i. Mobile and Deployable Contingency Communications. The CAMS maintain the CG's contingency communications assets that provide temporary communications capabilities in support of COOP and other emergent requirements. These assets may deploy on short notice and provide a wide array of communications support including radio (HF, UHF, and VHF), military and commercial voice and data satellite communication, and R21

disaster recovery system (DRS) equipment. Various packages of communication and interoperability solutions can be deployed to support Homeland Security operations, SAR, law enforcement and sector operations. The assets may deploy at any time, if available, in support of COOP events and shall automatically be deployed if the CG Headquarters COOP Plan is activated and/or Continuity of Government Readiness Condition (COGCON) 2 or 1 is set. Requests for contingency services must be submitted through the operational commander via the appropriate area/district as outlined in LANTCOMMSYS/PACCOMMSYS series record messages and district supplements.

j. Communication Area Master Station (CAMS) Back-Up Communication Area Master Station (CAMS) (CBUC). The goal of each CAMS is to provide highly reliable communication services to meet the needs of their customers. CAMSLANT and CAMSPAC have limited capability to transfer control of communications assets to the other CAMS during emergencies or unscheduled outages.

k. Communication Area Master Station (CAMS) Distress & Safety Statistics. Because distress and distress related safety communications normally relayed by a CAMS or COMMSTA Kodiak do not go directly to the watchstander responsible for SAR cases, relevant statistics regarding the specific method of communications is not captured by MISLE. Therefore CAMS and COMMSTA Kodiak shall be responsible for maintaining distress and safety statistics. Statistics shall be compiled annually and maintained for a period of 5 years. Annual calendar year statistics shall be provided to Commandant (CG-65) and Commandant (CG-534) upon request to enable evaluation of system performance. Reports shall include:

(1) Numbers of distress alerts received by MF/HF voice, except those initiated by DSC;

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

(3) Numbers of routine (non-safety related) calls received by MF/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 obviously incorrect;

(8) Number of DSC distress alerts which had a Maritime Mobile Service Identity (MMSI) which was obviously incorrect;

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

(10) Number of DSC test calls received.

E. Area and District Command Center (CC)/Sector Command Center(SCC)/Small Boat Station/Air Station (AIRSTA).

1. Area and District Command Center (CC). CCs function as the focal point for control of CG forces. CCs are staffed with personnel that have the necessary skills and expertise to ensure safe and effective operations. CC watchstanders require direct communication capabilities with DOD organizations, federal agencies including DHS, state and local officials, and the general public. Operational commanders specify requirements for communication facilities located in the CC.

   a. Commandant policy requires that all operational telephone circuits shall be terminated in the CC.

   b. CC watchstanders shall have classified, protected and non-classified voice communication capabilities with on-scene coordinators.

   c. Operational telephone and voice radio circuits (non-classified and protected only) shall be continuously monitored by means of electronic recording devices.

2. Sector Command Center (SCC). The SCC provides unified command and control, and serves an operations integration and coordination function. Each SCC shall be located organizationally to support response and prevention operations. The SCC includes a continuously staffed command and control watch with sole responsibility for monitoring, coordinating and maintaining tactical control of all CG and other agency assets in the sector's assigned AOR. Sectors are primarily responsible for communications within sea area A1 and A2; for specific sector communication guard requirements, refer to Chapters 10 and 11 of this Manual.

3. Small Boat Station. CG small boat stations operate VHF/FM low sites for local command and control of forces and logistics purposes. Some small boat stations are equipped with MF/HF where necessary to ensure boat crew communications and SAR monitoring. Stations equipped with MF/HF capability shall monitor 2182 kHz per Chapter 10 if equipment is not otherwise employed.

4. Air Station (AIRSTA). A CG AIRSTA is provided access to a communication capability either through the respective area COMMSYS or through its own facilities to communicate (normally within UHF/VHF range) with its aircraft and other mobile units. Access to communication capability shall be provided to enable each aircraft to operate safely and efficiently to its maximum radius of

operation. Some AIRSTAs are equipped with MILSATCOM where necessary to ensure flight safety. Normally, the requests for the installation of maritime mobile VHF- FM equipment or authorization for maritime mobile frequencies at CG AIRSTA's to support air-to-ground communication are not approved.

5. Vessel Traffic Service (VTS). VTS provide active monitoring, information, and navigational advice for vessels in particularly confined and busy waterways. VTS uses a variety of sensors (e.g., radar, Automatic Identification System (AIS) and closed circuit television) to monitor vessel traffic in the VTS area. The VHF-FM communications network is the basic and most important part of a VTS. Transiting vessels make position reports to the VTS by radiotelephone and are in turn provided with accurate, complete, and timely navigational safety information. The addition of AIS, radar and other surveillance tools combined with computer-assisted tracking allows the VTS to actively manage vessel traffic, with the aim of decreasing vessel congestion, reducing critical encounter situations, and preventing marine casualties resulting in environmental damage.

F. Coast Guard (CG) Auxiliary (AUX) Communication.

1. Auxiliary (AUX) Communication Network. The CAMS are responsible for control of the CG AUX communication network. This includes such activities as training and drills. AUX facilities may use one or more frequencies designated by the area commander, district commander, CAMS or by Commandant (CG-65) for specific authorized AUX activities. These activities include, but are not limited to: contingency communications, continuity of operations, quality control, and regattas. Further information regarding AUX communications and operations can be found in the Auxiliary Operations Policy Manual, COMDTINST M16798.3 (series).

   a. Keyed Very High Frequency-Frequency Modulated (VHF-FM) and Ultra High Frequency (UHF) Handheld Radios. CG Aux is authorized to use type-3 (SBU) keyed VHF-FM and UHF handheld radios to support CG operations. Units are authorized issuance of keyed handheld radios to CG AUX personnel. Prior to issuing keyed handheld radios to CG AUX, ensure that AUX's:

      (1) Are qualified as CG AUX communications operator per local unit requirements;

      (2) Operate keyed radios per approved Annex K to Area OPLAN district supplement and local SOPs;

      (3) Operate the radio only while under CG orders;

      (4) Possess a favorable operational support personnel security investigation and signed COMSEC Material System (CMS) User Acknowledgement Form on file;

      (5) Have a signed non-disclosure agreement (DHS Form 11000-6) on file;

(6) Have a letter on file signed by the CG orders issuing authority authorizing use, possession and custody of keyed handheld radios;

(7) AUX personnel shall complete unit training in keyed radio operations, storage, transportation, reporting loss/stolen keyed radios, and OTAR capabilities/operation;

(8) AUX personnel shall not maintain custody of physical KEYMAT or physical loading devices;

(9) AUX personnel shall not maintain personal custody of keyed radios unless specifically authorized to do so in section F.2.f. of this Chapter;

(10) The loading of KEYMAT in radios distributed to CG AUX personnel shall be limited to authorized CG personnel at the CG unit to which assigned or at an authorized CG support unit; and

(11) Authorization to load KEYMAT may be assigned to another CG unit on a limited case-by-case basis only.

G. Telecommunication Facility Design Requirements. A telecommunications facility is where the primary function of that space is to support CG telecommunications and includes: 1) all installed electrical and electronic wiring, cabling, and equipment, and 2) all supporting equipment such as utility, ground network, and electrical. CG telecommunication facilities shall be designed to provide efficient use of assigned personnel for circuit and network management, supply record message processing capabilities, and comply with security regulations. Designs for all new and rehabilitated facilities, including all site layouts, buildings, and government furnished equipment, shall comply with Civil Engineering Manual, COMDTINST M11000.11 (series), and Shore Facilities Standards Manual, COMDTINST 11012.9 (series).

1. Facility Security. The Physical Security and Force Protection Program, COMDTINST M5530.1 (series) and the Classified Information Management Program, COMDTINST M5510.23 (series) shall be consulted for all aspects of facility security. In particular, classified information processing functions and personnel traffic flow patterns shall be considered when designing communication spaces. Labels for rooms and equipment shall be as per the Electronics Manual, COMDTINST M10550.25 (series).

   a. Communication equipment necessary for the proficient operation of the telecommunication facility should be located within a secure space and under the supervision of operations or SCC/CC personnel. If space limitations make this unfeasible, communication equipment (less cryptographic equipment) should be located in spaces both adjacent and convenient to the operations or SCC/CC.

   b. Facilities with secure on-line communication capability shall be constructed as one secure room where both secure and non-secure processing equipment can be located.

c. TEMPEST requirements and design specifications for CG telecommunication facilities, cutter, and aircraft shall be per U.S. Coast Guard TEMPEST Program, COMDTINST M2241.6 (series). Contact the C4ITSC for current TEMPEST policy and guidance.

2. Emergency Power at Shore Facilities. Normal redundancy in CG communication exists through its capacity for redistribution. Emergency power and/or an uninterruptable power supply (UPS) shall be installed to operate mission essential equipment (CGOne, servers, hubs, routers, and radio equipment) in the event of commercial power failures at all units ashore having a direct responsibility for continuous service. Requests for new mission essential emergency power equipment shall be submitted to the SILC for funding/execution. New telecommunication facilities shall be designed with a back-up power supply. Emergency power procedures shall be outlined in area, district and sector COOP plans. Requirements and specific guidelines for emergency power are as follows:

   a. Generator capacity shall be adequate to permit operation of essential communication related equipment and must be capable of operating for a minimum of 72 consecutive hours without refueling.

   b. The emergency power supply at all CG shore telecommunications facilities shall be capable of automatic operation within 60 seconds after failure of commercial power, and must be sufficient to provide full operation of all necessary communication equipment and lighting in the areas of the CC or operations deck and where communication personnel are working. Further, the emergency power supply must be sufficient to provide simultaneous operation of equipment as determined by the operational commander.

   c. Communication and computer equipment sensitive to power fluctuations or has volatile random access memory (RAM) holding essential information required to permit continuous operation or rapid restoration shall be protected with an appropriately load-rated UPS. The UPS shall provide power for a minimum of 30 minutes. All telecommunication facility emergency power supply systems shall be tested as per COMDTINST M11000.11 (series), Civil Engineering Manual.

   d. Additional information concerning maintenance of generators is contained in the Electronics Manual, COMDTINST M10550.25 (series).

3. Large Electronic and Computer Installations. Facilities that host electronics or computer equipment, used to support CG telecommunications, shall conform to the construction and fire protection requirements as per National Electrical Code (NEC) and National Fire Protection Association (NFPA) publications.

CHAPTER 8 VESSEL TELECOMMUNICATIONS

A. Shipboard Communication Watches.

1. General. A primary duty assigned to OSs onboard cutters is communication watches. Depending on the size, location, and mission of the cutter the commanding officer is required to issue instructions to implement communication watch requirements as per the Cutter Organization Manual, COMDTINST M5400.16 (series). Unit specific communication SOPs shall be created and approved by the commanding officer. Communication SOPs shall be updated at least annually to remain current with communication staffing requirements on cutters.

2. Communication Watch Requirements. CG cutters are billeted as per the Personnel Allowance List (PAL). Watch requirements shall be as per the following guidelines:

   a. Three or more OSs. Maintain a continuous communication watch while underway, at anchor, or moored where landline communication is not available.

   b. Two or fewer OSs. Watches shall be scheduled per the current edition of ITU Radio Regulations while underway, at anchor, or moored where landline facilities are not available. The servicing CAMS shall be kept informed of the actual watch hours. This does not relieve the vessel of frequency guard requirements per Exhibit 8-1.

   c. Cutters in Port. Watches are not required when moored at home port or when the cutter is in maintenance and repair ("Charlie") status. When moored away from home port, communication watches shall be at the discretion of the operational commander if the cutter has shifted their communication guard to another unit. To meet the speed of service objective (Chapter 10 of this Manual), an underway cutter moored away from homeport that has not shifted their communication guard shall maintain a continuous communications watch to include monitoring record message traffic.

   d. Cutters Traveling in Company. Cutters may share the communication guard when traveling in company.

3. Visual Watch Requirements. The specific assignment of personnel as visual communication watchstanders shall be at the discretion of the commanding officer or as directed by the operational commander. The extent of training received by bridge watchstanding personnel shall be such that the cutter is capable of responding to all forms of visual communication (e.g., flags, semaphore) for which it is equipped.

B. Radio Frequency Guard Requirements.

1. Guard frequencies for cutters are based on laws, regulations, treaties, or international agreements, the requirements of the operational commander, the number of OSs assigned onboard, and the mission of the cutter. If a cutter is not suitably manned, the operational commander shall be notified and corrective action initiated. Cutters without an OS assigned are still required to maintain the minimum frequency guards per Exhibit 8-1. 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." During a continuous guard, the operator shall monitor the required frequency unless required to transmit on another frequency. After transmission, the operator shall immediately switch back to the guarded frequency. During an uninterrupted guard the operator can switch to another frequency to make a transmission, but shall not stop monitoring the frequency requiring an uninterrupted guard.

Exhibit 8-1
Minimum Radio Frequency Guards on CG Cutters

Class	**2182 kHz Note 1, 3**	**MF/HF 2187.5 kHz (DSC) Note 4**	**121.5 MHz 243.0 MHz**	**VHF-FM Channel 70 (156.525 MHz) (DSC)**	**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	X	X
WHEC	X	X	X	X	X	X	X	X
WAGB	X	X		X	X	X	X	
WMEC	X	X	X	X	X	X	X	X
WMEC Mature Class	X	X	X	X	X	X	X	X
WIX, WLB	X	X		X	X	X	X	
WLM	X			X	X	X	X	
Vessels 110' and larger, except WLIC	X			X	X	X	X	X
Vessels under 110' and over 26'				X	X	X	X	X
Vessels under 26'	As Required by the operational commander							

Note 1: Frequency guard required by someone on the vessel (e.g., bridge, combat information center (CIC), radio).
Note 2: Frequency guard as dictated by the operational commander.
Note 3: When operating in the Alaskan AOR, cutters shall also guard 4125kHz.
Note 4: If equipped.

2. Under special circumstances, the operational commander may authorize deviations from exhibit 8-1 on a temporary case-by-case basis to meet operational requirements. In granting exceptions, the operational commander shall take into

consideration that many of the guards listed are required by law, international treaty, or agreement.

3. Voice radio guards shall be maintained on the bridge and/or CIC. The unit communication plan shall ensure all required frequency guards are appropriately allocated between the bridge and CIC.

C. Vessel Bridge-to-Bridge Radiotelephone Act.

1. Applicability. Commanding officers, officers-in-charge, and conning officers shall be familiar with the Vessel Bridge-to-Bridge Radiotelephone Act (33 U.S.C. §§ 1201-1208; CG Regulations implementing the act are in 33 C.F.R. §§ 26.01-26.09). The Act is applicable on navigable waters of the United States inside the boundary lines established in 46 Code of Federal Regulations (C.F.R) Part 7. The Bridge-to-Bridge frequency is 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. The following CG cutters shall participate:

   a. Cutters 65 feet or longer while operating upon the navigable waters of the United States; or

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

2. Interpretation. The Act's regulations state in part that 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 CG policy purposes, this may be the commanding officer, officer-in-charge, conning officer, officer-of-the-deck (OOD) (if actually directing the movement of the vessel - has conning officer duties), or pilot (if applicable). This function cannot be delegated to others. All Bridge-to-Bridge communications must be conducted in the English language.

   a. All cutters shall 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.

   b. The Bridge-to-Bridge radiotelephone frequency is to be used only to transmit and confirm the intentions of the vessel and any other information necessary for safe navigation.

   c. Failure of the installed Bridge-to-Bridge radiotelephone(s) alone is not sufficient cause for non-participation. When a need arises, a portable radio may be used as the Bridge-to-Bridge radiotelephone.

d. Unless the normal use of the Bridge-to-Bridge radiotelephone installation demonstrates that the equipment is in proper operating condition, a test communication for this purpose shall be made prior to getting underway and each day that the cutter is navigated. If the equipment is not in proper operating condition, the commanding officer shall be notified immediately.

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

f. The transmitter used on the designated Bridge-to-Bridge frequency is limited to 1 watt or less output power for normal operations and, when necessary, shall not exceed 25 watts for ship stations and 10 watts for shore stations. Portable radio equipment may be used.

g. 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.

h. A voice log is required for CG cutters only if that class of cutter is required to maintain a radio log as per Chapter 6 of this Manual. One log may be used to record all VHF-FM transmissions. A non-CG operational commander may require separate logs while a cutter is under its control.

D. Cutter Communications.

1. Communication Guard Shift (COMMSHIFT). Cutters shall submit a COMMSHIFT each time prior to transferring their telecommunication guards and record message delivery responsibilities from one communication facility to another. A cutter shifting its guard to a USN unit shall submit a COMMSHIFT record message as per Pre-Formatted (PROFORMA) Message Handbook, NTP 4 SUPP-2 (series). Mobile units/ shifting their guards to their servicing CAMS shall refer to the applicable LANTCOMMSYS/ PACCOMMSYS series record messages for procedures and record message formatting guidance. 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. Mobile units deploying for less than 72 hours are not required to submit COMMSHIFT record messages unless shifting to a USN unit. COMMSHIFTs not placed into effect result in missed record messages for the submitting command. Therefore, commands shall contact the appropriate guarding facility to ensure their submitted COMMSHIFT record message has been received prior to the COMMSHIFT taking effect. Guidance for underway record messaging is provided as follows:

a. Cutters shifting their record message guards to NCTAMS facilities for messaging shall be guided by the provisions of Telecommunications User Manual, NTP 3 (series) and Communication Information

Bulletins/Communication Information Advisories (CIBs/CIAs). Cutters shall maintain copies of these publications, electronically (e.g., Coast Guard standard workstation (CGSW)) or on paper, at all times due to limitations of underway connectivity to CGOne.

b. Cutters maintaining their record message guards with their CAMS shall be guided by this publication, Annex K to Area OPLAN, district supplement, and LANTCOMMSYS/PACCOMMSYS series record messages. Cutters shall maintain copies of these publications, electronically (e.g., CGSW) or on paper, at all times due to limitations of underway connectivity to CGOne.

E. Communication Spot (COMSPOT) Report. COMSPOT reports shall be submitted by all cutters whenever unusual communication difficulties (e.g., lost communications, equipment failure, interference) are encountered. Cutters shall submit the COMSPOT to the terminating shore facility. Refer to Appendix C of Fleet Communications, NTP 4 (series) for further details.

1. Naval Computer and Telecommunications Area Master Station (NCTAMS) Termination. Cutters with terminations with a NCTAMS shall submit COMSPOT reports action to NCTAMS, information to the CAMS and area. Exhibit 8-2 is an example of a COMSPOT report from a cutter terminated with NCTAMS.

Exhibit 8-2
COMSPOT Report from Cutter Terminated With NCTAMS

P 151800Z JAN 12
FM USCGC MELLON
TO NCTAMS PAC HONOLULU HI
INFO COGARD CAMSPAC PT REYES CA
COMPACAREA COGARD ALAMEDA CA//PAC-6//
BT
[CLASSIFICATION AS REQUIRED] //N02318//
MSGID/COMSPOT/USCGC MELLON//
SUBJ/COMSPOT//
RMKS/1. SHIP'S POSITION OR PORT NAME.
2. DESCRIPTION OF PROBLEM, FREQUENCY (IF APPLICABLE), AND STATION INVOLVED. DESCRIBE CORRECTIVE ACTION TAKEN BY UNIT.
3. RECOMMENDED SOLUTION OR REQUEST ADVISE.
DERIVED BY/DECLAS://
BT

2. Communication Area Master Station (CAMS) Termination. Cutters with terminations at CAMS shall submit COMSPOT reports to the CAMS, information to the appropriate area/district/parent command. Exhibit 8-3 provides an example of a COMSPOT report from a cutter terminated with CAMS.

Exhibit 8-3
COMSPOT Report from Cutter Terminated With CAMS

P 151900Z JAN 12
FM USCGC DAUNTLESS
TO COGARD CAMSLANT CHESAPEAKE VA
INFO COMLANTAREA COGARD PORTSMOUTH VA// LANT-6//
BT
[CLASSIFICATION AS REQUIRED] //N02318//
MSGID/COMSPOT/USCGC DAUNTLESS//
SUBJ/COMSPOT//
RMKS/1. SHIP'S POSITION OR PORT NAME.
2. DESCRIPTION OF PROBLEM, FREQUENCY (IF APPLICABLE), AND STATION INVOLVED. DESCRIBE CORRECTIVE ACTION TAKEN BY UNIT.
3. RECOMMENDED SOLUTION OR REQUEST ADVISE.
DERIVED BY/DECLAS://
BT

3. Precedence Assignment. Precedence assigned to COMSPOT reports may be routine, priority or immediate, as required by operational needs.

F. Command Guard List (COMMGRDLST). The COMMGRDLST is used by mobile units to determine record message guard requirements. Commanding officers are responsible for maintaining an accurate guard list of Address Indicating Groups (AIGs), Collective Address Designators (CADs), and Task Organization assignments of which they are members. Cutters shall request and review their guard lists prior to deployment and update as necessary. Refer to Pre-Formatted (PROFORMA) Message Handbook, NTP 4 SUPP-2 (series) for further guidance. Ensure the applicable CAMS are an action addressee on all guard list requests, submittals, and modifications.

G. Boat Communications.

1. Operations Normal Reports. Operations Normal (Ops Normal) reports are required for all boats as defined in the Boat Crew Seamanship Manual, COMDTINST M16114.15 (series). Underway boats are required to provide an operations status report every 30 minutes for small boats and every 4 hours for all other boats, unless otherwise established by local command SOPs. The information in the report shall contain current position, operational status, and significant changes in weather, wind, and sea conditions. The operational commander may modify required reporting information if a situation dictates.

   a. Shore stations losing contact with a boat must attempt to reestablish communication directly with the boat or through another station. If no communication is established, a lost communication record message shall be initiated. Chapter 9 of this Manual contains an example record message (lost communications with an aircraft) that can be used as guidance. Area and

district commanders may publish additional policy for alert procedures in lost communication situations.

b. Normal operations status reports shall be transmitted as "Ops normal".

c. Any communication with a boat shall serve to begin a new period for the purpose of making the next operations status or position report.

d. Operations status that is other than normal shall be reported accordingly.

2. Exemptions from Ops Normal Reports. Boats/cutters underway and operating under the following conditions are exempted from operations status or position report requirements with a shore facility:

a. When maintaining communication with the on-scene coordinator in conjunction with a SAR mission. The boat/cutter shall make the required reports to the on-scene coordinator. A boat/cutter engaged in a SAR mission and reporting to an on-scene coordinator should shift its telecommunication guard to the on-scene coordinator until released from the SAR mission; or

b. When instructed by proper authority to maintain radio silence. In any case of contemplated radio silence, the shore facility shall be so advised and radio contact reestablished as soon as practicable.

H. Visual Communication Procedures.

1. General Visual Procedures. Use the procedures found in the International Code of Signals (INTERCO) (for visual, sound, and radio communication), National Geospatial-Intelligence Agency (NGA) Pub. 102, shall be used when exchanging calls with ships of unknown registry, merchant ships, and non-allied ships.

a. Many of the pro-signs prescribed for visual signaling between allied naval vessels in Communications Instructions Signaling Procedures in the Visual Medium, ACP 130 (series) are either not recognized in NGA Pub. 102 or have different meanings and shall not be used when signaling non-allied naval ships and ships of unknown registry. It is possible that a serious international situation could result through misinterpretation.

b. When the identity of a ship has been 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) may be used provided no possible confusion could arise onboard other vessels in the vicinity.

2. Flashing Light. Directional flashing light is the term applied to the transmission of signals by a narrow beam of light such as a signaling searchlight. Non-directional flashing light is the term applied to the transmission of signals in all directions by a signal light such as a yardarm blinker. To reduce the probability of interception, directional flashing light shall be the primary method of flashing

light communication. Non-directional flashing light shall be considered the secondary means of flashing light communication, and may be used in situations where the signaling unit desires to signal more than one addressee at a time.

a. Between sunset and sunrise 12 inch searchlights shall be fitted with a suitable filter and a reducer, except when use of unfiltered light is necessary. When using colored filters, due consideration shall be given to the following:

   (1) Use only red filters to avoid reducing the receiver's night vision; and

   (2) Use red or green filters with caution so as to not override or be mistaken for the sidelights of a ship when underway.

b. 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 translates to "The following is to be taken as applying to personnel on watch only." Although there should normally be no objection to such unofficial signaling in peacetime, such signals shall not be originated or answered without the permission of the commanding officer.

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

4. Maintenance of Visual Records. When maintaining a visual signal watch, units shall maintain a visual communication record as per Chapter 6 of this Manual.

CHAPTER 9 AIRCRAFT TELECOMMUNICATIONS

A. Scope and Applicability. Unique support requirements involving new resources for aircraft shall be determined by area and district commanders and approved by Commandant (CG-711). All CG aircraft shall follow the principles and forms of communication prescribed in this Manual, Radiotelephone Handbook, COMDTINST M2300.7 (series), pertinent ACPs, JANAPs, CG LANTAREA and PACAREA Instructions, International Civil Aviation Organization (ICAO), and FAA publications, FCC policy and ITU policies, treaties and agreements.

B. General.

1. CG aircraft shall establish a communication guard with an aeronautical facility within 5 minutes after takeoff. An aeronautical facility is defined as a land station in the aeronautical mobile service and includes civilian air traffic controls (ATC), CG stations, or other military facilities. Generally, CG aircraft should maintain their primary operational communication guard through a CG facility.

2. Where geographically and economically practicable, area COMMSYS facilities shall be used for medium and long-range HF air-to-ground support. Local operations, including taxiing, fire/crash truck dispatch, etc. shall be conducted on UHF and/or VHF-FM over non-maritime mobile bands.

3. 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 will not normally be approved.

C. Communication Guard Requirements.

1. The aeronautical station accepting the guard for the aircraft shall 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.

2. When a communication guard is accepted by a CG unit, the unit accepting the guard will ask the aircraft commander how many persons are onboard, where the flight originated, destination and hours of fuel remaining.

3. The CG unit accepting the guard will provide primary and secondary frequencies, the next scheduled communication check and following communication checks thereafter.

4. While in flight and operations permitting, all CG aircraft shall guard the following emergency frequencies:

   a. 121.5 MHz;

   b. VHF-FM Channel 16 (156.800 MHz); and

c. 243.0 MHz.

5. The use of these frequencies shall be restricted to emergency communication or situations where other frequencies will not suffice. Normal communication shall be conducted on the appropriate CG or aeronautical unit's working frequency.

6. If a change of communication guard is necessary due to operations and/or deteriorating communications, the aircraft must ensure the unit maintaining primary guard is immediately notified via any method. Failure to do so will result in lost communications procedures being implemented and unnecessarily diverting all communication assets in the area as they try to reestablish contact with the aircraft.

D. Reporting Requirements. AIRSTAs will normally receive medium and long range air-to-ground support from the area COMMSYS.

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

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

(1) Normal flight operations status reports shall be transmitted as "flight ops normal", or

(2) Operations status that is other than normal shall be reported accordingly.

b. Rotary – Helicopters. A flight operations status report every 15 minutes and a position report every 30 minutes.

(1) Normal flight operations status reports shall be transmitted as "flight ops normal", or

(2) Operations status that is other than normal shall be reported accordingly.

2. Each position report shall include course, altitude and speed. Any communication between an aircraft and its communication guard station will serve to begin a new period for the purpose of making a required report.

3. When the aircraft is maintaining communication with ATC facilities, the required reports shall be made as per current FAA regulations. Whenever possible, the aircraft commander shall also maintain a guard on CG frequencies to the extent that it will not interfere with the primary ATC communication.

4. When the aircraft is maintaining communication with an on-scene coordinator or officer-in-tactical command (OTC) in conjunction with a coordinated mission, the aircraft commander shall make the required position reports to the on-scene coordinator or OTC. An aircraft engaged in a coordinated mission and reporting to an on-scene coordinator/OTC should shift its communication guard from the

aeronautical unit to the on-scene coordinator/OTC until released from the coordinated mission.

5. When the aircraft has been instructed by proper authority to maintain radio silence, the requirement to maintain a communication schedule with an aeronautical unit is waived. The aeronautical unit shall be so advised and radio contact reestablished as soon as practicable.

6. If an aeronautical station loses contact with an aircraft, it is the responsibility of the guard station to initiate the necessary actions to re-establish communication with the aircraft directly or through another unit, or to initiate an alert.

7. When the aircraft's mission is complete or when the communication guard is transferred to another unit, the aircraft commander shall notify the losing unit to secure the guard. Failure to notify a guarding unit of their intentions will cause the unit to issue a lost communication alert.

8. CG aircraft in receipt of a DSC alert shall, if operations permit, immediately acknowledge the alert and relay the pertinent information to their operational commander via the most expeditious means available.

E. Lost Communication.

1. If the aircraft commander fails to check in on the primary or secondary frequencies within 5 minutes of the communication schedule, the guarding unit shall initiate an alert. The aircraft's parent command shall be notified first, followed by the cognizant district CC. If the aircraft is not located, an immediate precedence record message shall be sent. An example of a lost communication report for aircraft is in Exhibit 9-1.

Exhibit 9-1
Lost Communication Record Sample Message

(Date-time-group)
FM (Unit reporting lost aircraft communication)
TO (all communication units/cutters within the AOR the aircraft was operating in)
(Aircraft's parent command)
INFO (Appropriate area CC)
(Cognizant district CC)
BT
UNCLAS FOUO //N02000//
SUBJ: LOST COMMS REPORT
1. ORIG LOST COMMS WITH COGARD AIRCRAFT (tail number). LAST COMMS ON (appropriate frequency). LAST POSITION (latitude/longitude).
2. REQ RADIO EQUIPPED UNITS ATTEMPT COMMS AND ADVISE.
3. REQ ALLSTA ADVISE IF COMMS ESTABLISHED ON VHF/UHF/HF EQUIPMENT OR VIA OTHER MEANS.
4. ORIG WILL ADVISE ALL ADDEES WHEN COMMS REESTABLISHED.
BT
NNNN

2. When communication is reestablished with the aircraft, an immediate precedence record message will be sent to all addressees listed in lost communications report with notification that communication has been restored and the reason for lost communication.

F. Frequency Selection.

1. Very High Frequency/Ultra High Frequency (VHF/UHF). VHF and UHF air-to-ground frequencies shall be used to the fullest extent possible for short-range communication with the aircraft's parent command. CG VHF and UHF maritime mobile frequencies may be used to communicate with CG small boats and sector shore units.

   a. In emergencies or SAR situations CG aircraft may use any frequency authorized to a non-government facility. Commanding officers should determine what VHF-FM frequencies are used by public safety agencies in their area and submit requests for use as per Spectrum Management Policy and Procedures, COMDTINST M2400.1 (series).

   b. VHF-FM Channel 83 (157.175 MHz) shall not be used in the areas where interference with Canadian users of this frequency could occur unless experiencing an in-flight emergency.

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

   d. Aircraft operating above 1000 feet shall not transmit on VHF-FM maritime channels (frequency range 156-162 MHz) with the exception of reconnaissance aircraft participating in icebreaking operations which may operate on these channels up to an altitude 1500 feet. Transmissions by aircraft in this band shall not exceed 5 watts. In the event there is a safety related situation, an aircraft operating above 1000 feet may communicate on these channels provided the communication is as brief as possible and the communication is not likely to cause interference to other communications.

      Note: The safety of life and non-interference exceptions is at the determination of the pilot. In making this determination, the pilot shall 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 may 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.

   e. 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.

f. Aircraft may broadcast urgent maritime safety information and weather warnings to ships. District commanders shall determine policy on broadcast content and when such broadcasts are necessary. No transmission on VHF-FM Channel 16 (156.800 MHz) shall be made unless that frequency is monitored from the aircraft and determined to be clear of distress and safety communications. Transmission duration on VHF-FM Channel 16 (156.800 MHz) shall be short and in no cases exceed 60 seconds. Deviation from the requirements of sections F.1.c. and F.1.d. of this Chapter is permissible only when necessary to protect safety of life. Appropriate sector watchstanders and foreign rescue coordination centers shall be notified, where appropriate, before commencement of broadcasts.

2. High Frequency (HF). CG HF air-to-ground frequencies shall be used for long range communication with a CAMS or COMMSTA Kodiak. Commandant (CG-652) hosts a frequency database to provide users with unit specific frequency authorizations. This can be found on the communications portal at: http://cgweb.rss.uscg.mil/communicationsportal/.

   a. Secure Air-to-Ground (SAG). SAG is a secure air-to-ground network designed for aircraft to communicate with a CAMS or other command when information pertaining to the aircraft's mission must not be passed in the clear. Refer to LANTCOMMSYS/PACCOMMSYS series record message for specific procedures and frequencies regarding SAG.

   b. Cellular over the Horizon Enforcement Network (COTHEN). CG aircraft use COTHEN as a primary means to maintain reliable communication with CAMS (see Chapter 7, section D.4.C of this Manual).

   c. Geo-Spatial over the Horizon ALE Matrix (GOTHAM). COMMSTA Kodiak operates GOTHAM to provide both clear and secure aircraft communication (see Chapter 7, section D.4.C of this Manual).

3. Wulfsberg RT-5000 Very High Frequency/Ultra High Frequency (VHF/UHF) Code Plugs. To achieve the CG operational goal of seamless intraoperable communications between CG radios and interoperability with federal, state and local partners, the RT-5000 code plug and RPWIN files requires a single management organization. Enterprise management of the standard aviation code plug is necessary to ensure aviation platforms throughout the CG have the same baseline code plug as any other CG mobile platform (e.g., vessels, vehicles, handheld radios). Having the standard code plug loaded in aviation platforms ensures that frequencies and naming conventions conform to all other portable and mobile supported CG radios. All commands shall comply with the enterprise frequency plan.

a. The C4ITSC is responsible for the development, maintenance, and tier-3 support for the CG standardized code plug code plug and RPWIN files for all RT-5000 tactical radios. The standard code plug is developed per telecommunication policies and standard CG-wide frequency plans established by Commandant (CG-65). Units are required to maintain these standard code plugs and RPWIN files in the RT-5000 consistent with System Management and Engineering Facility (SMEF) or Technical Bulletin record messages published by the C4ITSC.

b. CG districts shall add local district/sector requirements to the CG-wide standard code plug called Zones of Convenience. Since aviation assets use preset channels, there is no need to create redundant channels in a district Zone of Convenience. The local ESU and ESD are responsible for developing, maintaining, and providing RT-5000 code plugs and RPWIN files to support local frequency requirements and will add approved district local frequencies to the standard aviation code plug and RPWIN files.

c. Operations and maintenance personnel are authorized to download the standard C4ITSC baseline code plug, RPWIN and district modified code plug and RPWIN files. RT-5000 operations and maintenance personnel are not authorized to make modifications to or deletions from the standard frequency, channel or naming scheme in the C4ITSC baseline code plug and RPWIN files. Requests for modification will be submitted to the district (dt) for approval. Code plug and RPWIN files are thoroughly tested and operational evaluations are conducted periodically. Code plugs and RPWIN files are available for download at: http://cgweb.rss.uscg.mil/communicationsportal/default.aspx.

d. To comply with national policy and maintain enterprise COMSEC standards, the RT-5000 system will use AES standard on all SBU circuits. DES standards will be used for interoperability with legacy systems as required. The CBP NLECC provides centralized key generation, management, and distribution of the RT-5000 cryptographic KEYMAT. Centralized control over encryption keys reduces procedural, operational, and security problems and assures the integrity of the keys.

G. Call Signs. Voice call signs for aircraft shall be as per Radiotelephone Handbook, COMDTINST M2300.7 (series) and appropriate instructions issued by the operational commander. All aircraft on SAR missions and desiring expeditious handling by the FAA shall insert the word RESCUE in the call sign after CG when using voice procedures.

H. Record Messages.

1. The responsibility for filing record messages rests solely with the aircraft commander. It is the responsibility of the aircraft commander to ensure the commanding officer of such ship or station that is the point of departure or arrival is properly notified as to such movement, departure, or arrival.

2. Aircraft commanders, when originating a record message, will use the PLA of the aircraft's parent command followed by the aircraft number (e.g., COGARD AIRSTA ELIZABETH CITY NC//CGNR 2131//). When an aircraft changes its operational control ("CHOP") to another command the same instruction applies using the operational commander's PLA. The aircraft's parent command will be included as an addressee to the record message. Sample record message headings from CG aircraft appear in Exhibit 9-2.

Exhibit 9-2
Record Sample Message Headings from CG Aircraft

From Parent Command: FM COGARD AIRSTA ELIZABETH CITY NC//CGNR 2131// TO CCGDFIVE PORTSMOUTH VA//DXO// INFO COGARD AIRSTA ELIZABETH CITY NC
From Operational Command: FM COGARD AIRSTA BORINQUIN PR//CGNR 2131// TO CCGDSEVEN MIAMI FL//DXO// INFO COGARD AIRSTA BORINQUIN PR COGARD AIRSTA ELIZABETH CITY NC

I. Aircraft Visual Communication Procedures.
Standard visual communication procedures for aircraft can be found in the Federal Aviation Administration (FAA) Aeronautical Information Manual (AIM).

CHAPTER 10 RECORD MESSAGING, E-MAIL, CHAT SERVICES AND TEXT

A. General. The policies in this Chapter apply to record messaging, E-mail, chat services and text.

B. Record Messaging. CG messaging is comprised of two systems: CG Messaging System (CGMS) and services provided by the USN. Policy and procedures for CGMS and record message format are as per Appendix B of this Manual, and appropriate Allied, Navy, and Joint publications. If this Manual conflicts with the policies outlined in the publications listed in section B.2 of this Chapter contact Commandant (CG-652) for clarification.

1. Inviolability of Record Messages. Distribution of record messages and the location of record message files shall prevent unauthorized viewing or access. Each command shall employ the following measures to protect record message files:

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

   b. Set restrictions on electronic record message boards;

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

   d. Do not forward record messages via E-mail or FAX to non-addressees simply for ease of providing others the same information. Record messages that are not received via the Coast Guard Record Messaging System (CGRMS) shall not be considered official record; and

   e. Internet releasable information via official CG record message. See section B.4 of this Chapter.

2. Telecommunication Library. All units preparing and transmitting record messages, shall maintain ready access to applicable publications at all times. CGOne provides online access to the full array of unclassified telecommunication publications listed below. Cutters must maintain either paper copies or electronic versions retrievable from onboard computers or stored off line on compact discs. The following publications are required for units using the CGRMS:

   a. Telecommunication Manual, COMDTINST M2000.3 (series);

   b. Communications General Instructions, ACP 121 (series);

   c. Allied Telecommunications Record System (ALTERS) Operating Procedures, ACP 128 US Supp-1 (series);

   d. Naval Telecommunications Procedures Navy Satellite Operations, NTP 2 SEC 1 (series) – WMEC-210' and above/CAMS/COMMSTA Kodiak only;

e. Navy Satellite Operations Sec II, NTP 2 SEC 2 (series) – WMEC-210' and above/CAMS/COMMSTA Kodiak only;

f. Telecommunications Users Handbook, NTP 3 (series);

g. AIG, CAD, TASK Handbook, NTP 3 SUPP-1 (series);

h. Fleet Communications, NTP 4 (series);

i. PROFORMA Message Handbook, NTP 4 SUPP-2 (series);

j. Spectrum Management Manual, NTP-6 (series);

k. C4I Infrastructure, NTTP 6-02 (series);

l. Operational Reports, NWP 1-03.1 (series); and

m. Navy Planning, NWP 5-01 (series).

3. Messaging Roles and Definitions.

a. Originator. The originator of a record message is the command by whose authority a record message is sent. The originator is responsible for the functions of the drafter and releasing officer.

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 the record message drafting instructions. Releasing authority is an administrative function of each command served by a record message center.

4. Internet Release of Record Messages. Record messages authorized for internet release shall have the following statement as the last line of text: "INTERNET RELEASE AUTHORIZED". For additional direction on internet release of CG Directives, refer to the Coast Guard Directives System, COMDTINST M5215.6 (series).

a. CAMSLANT is designated as the only authorized organization to post record messages to the internet. CAMSLANT will post internet releasable record messages as received via CGMS but are not responsible if unauthorized content is posted. Record message content is the responsibility of the record message originator.

(1) Internet released record messages shall only be posted on the following website by the designated CAMSLANT POC: http://www.uscg.mil/announcements.

(2) Record messages required to be publicly released that are not of general distribution nature (e.g., ALCOAST, ALCGENL) must also be addressed to CAMSLANT, otherwise the record message will not be posted. The PLA is: COGARD CAMSLANT CHESAPEAKE VA. For any questions concerning the need to include CAMSLANT, the 24/7 contact number is: (757) 421-6240.

(3) Once internet released information has been posted to the official website, individuals may distribute the posted information as they normally would if viewing other public internet sites.

b. CG information found via other internet sites (e.g., CG, public, private blog) may not be current or accurate and should not be used as a source of official CG information.

Note: For all CG internet web content managers: To avoid confusion and duplication, CG internet released record messages currently available on CG internet sites other than www.uscg.mil may remain but no new record messages shall be posted to such sites. Web managers of these sites are responsible for ensuring old/outdated CG record messages are promptly removed.

5. MINIMIZE. The commanding officer shall not permit release of non-urgent record messages when MINIMIZE is imposed. Record messages released during MINIMIZE must have as the last line of text "Released by (name and rank/grade)" as per Fleet Communications, NTP 4 (series).

6. Record Message Classes. There are three classes of government record messages handled by the record message system.

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

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

c. 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.

7. General Record Messages. General record messages are intended to meet recurring requirements for the dissemination of information to predetermined standard distribution.

a. Description. General record messages are entitled (e.g., ALCOAST, JAFPUB, ALPACFLT) and the title determines the distribution. Its members are the ACTION or INFORMATION addressees. General record messages

are assigned a consecutive three-digit serial number followed by a single slant and the last two digits of the current calendar year. General record messages are:

(1) All Coast Guard (ALCOAST). Releasing authority is restricted to the Commandant, Vice Commandant, Chief of Staff, Headquarters Flag/Senior Executive Service (SES) positions and those acting in that capacity. This release authority has been extended to LANTAREA and PACAREA Commanders and Force Readiness Command for service-wide matters under the authority of these positions. This authority cannot be further delegated.

(2) All Coast Guard officers (ALCGOFF).

(3) All Coast Guard enlisted (ALCGENL).

(4) All Coast Guard Personnel Service Center (ALCGPSC).

(5) All Coast Guard reserve (ALCGRSV).

(6) All Coast Guard civilian (ALCGCIV).

(7) All Coast Guard finance (ALCGFINANCE).

(8) All Coast Guard recruiting (ALCGRECRUITING).

b. Originators. General record messages may be originated by:

(1) Coast Guard (CG). Commandant, area and district commanders, Commander CG Personnel Service Center (except ALCOASTs as noted in section B.7.a.(1) of this Chapter);

(2) United States Navy (USN). CNO, Secretary of the Navy (SECNAV), Commander Naval Network Warfare Command (COMNETWARCOM), Commander Naval Security Group Command (COMNAVSECGRU), fleet, forces, and type commanders; and

(3) Joint. CJCS, Joint Staff, and Joint or Unified Commanders.

c. Preparing General Record Messages. Prepare general record messages in the same manner as an organizational record message, but enter the general record message title (or collective address) as an action addressee rather than individually listing each addressee. Add other addressees in the address lines as needed. Include in the record message text the general record message title, three-digit serial number followed by a slant and the last two digits of the calendar year following the classification line.

d. Retention and Cancellation. Record message cancellation is the responsibility of the originator. There are three methods used to cancel general record messages:

(1) For certain series of general record messages, the first general record message of a calendar year lists those record messages that remain effective. By omission, all general record messages of the series not listed are cancelled. If necessary, interim cancellation record messages may be sent at other times during the year.

(2) An individual general record message may include its own cancellation date within the text.

(3) General record messages of a series for which a yearly recapitulation record message is not issued are automatically cancelled at the end of 1 year. This period of time may be extended by a subsequent general record message of the same series within 1 year of the original record message and stating a date when the record message is to be cancelled. If 1 year has passed and no extension of time has been affected, a general record message must be reissued if it is to remain effective.

e. Review/Recapitulation. Originators shall continuously review their posted information for applicability throughout the year and immediately advise the CAMSLANT of any outdated information. Originators shall submit an annual recap of their effective record messages to the CAMSLANT no later than 31 January. After 31 January, all record messages older than one year but still effective will be moved to the "Effective Messages" portion of the site. Originators are still responsible to review the "Effective Messages" site and promptly advise CAMSLANT of any outdated information.

f. Retransmission. Units requiring CG, USN, and Joint general record messages can find them at: https://cgportal.uscg.mil/delivery/Satellite/HQCOMMS/.

g. Applicability and Distribution. Headquarters and area shall coordinate with CAMSLANT to ensure routing guard lists remain accurate for CG units.

8. Plain Language Addresses (PLAs). PLAs are unit identifiers which denote the command authority responsible for all content in a record message. A PLA normally has the command short title, occasionally followed by an identifying geographic area (e.g. COGARD CAMSLANT CHESAPEAKE VA). PLA requests normally conform to the Operating Facilities (OPFAC) of the U.S. Coast Guard, COMDTINST M5540.2 (series) but special circumstances will be considered on a case-by-case basis.

a. Send requests for establishing a PLA via the chain-of-command to CAMSLANT once an Operating Facility Change Order (OFCO) has been released authorizing creation of a unit.

b. PLA changes or requests for disestablishment shall be sent directly to CAMSLANT.

c. Do not exceed 50 characters (including geographic area) in a PLA.

9. Collective Addresses. The term "Collective Address" refers to the CAD, AIG, or Task Organization (TASK). Requests for changes to or the establishment of new CG CADs and AIGs shall be submitted to CAMSLANT.

   a. Collective Address Designator (CAD). A CAD is a single group that represents a predetermined set of activities linked by an operational or administrative chain-of-command.

      (1) A CAD is comprised of a minimum of 30 PLAs, and is used a minimum of 15 times per calendar year.

      (2) Make CAD assignment requests by record message to the cognizant authority through the normal chain-of-command.

   b. Address Indicating Group (AIG). An AIG is an address designator representing a list of specific and frequently recurring combination of ACTION and/or INFORMATION addressees. Any record message that is repetitively addressed to a consist group of thirty or more addressees, reflecting a community of interest can effectively be processed by use of an AIG address designator.

      (1) An AIG is comprised of a minimum of 30 PLAs, and is used a minimum of 15 times per calendar year.

      (2) Units may make AIG assignments requests by record message to the cognizant authority through the normal chain-of-command.

   c. Task Organization (TASK). TASK groups shall be established and maintained by individual units.

   d. Recapitulation. The cognizant authority is the commander responsible for the composition and use of the AIG/CAD. Cognizant authorities must recapitulate each AIG/CAD at least once per year or when 10 modifications have been issued and ensure that each AIG/CAD maintains a minimum of 30 members.

      (1) CAMSLANT's directory services manager is authorized to act in place of the cognizant authority for CG owned AIGs/CADs for the purpose of creation, modification, maintenance and disestablishment.

      (2) Cognizant authorities should route any changes to their AIGs/CADs through the directory services manager.

10. Staff Symbols. Staff symbols, also called office codes, 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 PLAs.

11. Exercise Record Messages. Identify exercise record messages by inserting the word "EXERCISE" three times below the record message's subject line, and the last line of text, as shown in Exhibit 10-1. Proper authority shall assign this identification. Commands or persons responsible for conducting exercises shall include appropriate instructions for identifying exercise record messages in the exercise directive or plan. Additionally, exercise record message instructions shall be clear to the reader concerning actions that should or should not be simulated.

Exhibit 10-1
Exercise Record Message Example

O XXXXXXZ JAN 12
FM COMLANTAREA COGARD PORTSMOUTH VA//LANT-00//
TO ALLCOGARDLANT
BT
UNCLAS FOUO //N02000//
SUBJ: (NAME OF EXERCISE)
EXERCISE EXERCISE EXERCISE
1. OPERATION XXXXXXX COMMENCES AT XXXXXXZ JUL 08 AND IS APPLICABLE FOR ALL LANTAREA UNITS. ALL ASPECTS OF THIS EXERCISE WILL BE SIMULATED UNLESS OTHERWISE DIRECTED BY THIS RECORD MESSAGE OR BY THE EXERCISE COORDINATOR.
EXERCISE EXERCISE EXERCISE
BT
NNNN

12. Standard Subject Indicator Code (SSIC). All naval record messages (record messages originated by USN and CG commands) require an SSIC (exceptions noted below). The SSIC is a four or five digit numeric code used to aid in the routing of official correspondence, including record messages, memoranda, Instructions, and Manuals. As used in record messages, the SSIC is appended to the classification line, preceded by a single space, double slant bar and the character N, and followed by a double slant bar, e.g., //N16130//. Four digit SSICs will include a leading zero to maintain a five-digit format for record messages.

    a. The following exceptions apply to this requirement:

        (1) Tactical record messages handled exclusively on tactical circuits;

        (2) Record messages using code or flag-words exclusively to identify the subject;

        (3) Record messages transmitted on dedicated or closed networks; and

        (4) CASREP, Movement Report (MOVREP), Status of Resources and Training System (SORTS) record messages, and record messages

containing the USN's portion of the Joint Reporting System (JRS). All other pro-forma record messages shall contain an SSIC.

b. The SSIC "//N00000//" may be assigned to high precedence record messages if determining the proper SSIC will delay the record message.

c. Since some commands use SSICs as a means to determine internal record message distribution, these commands should exercise care in selecting the SSIC that most accurately corresponds to the record message subject matter.

d. The Standard Subject Identification Codes (SSIC) Manual, COMDTINST M5210.5 (series) contains a complete list of SSICs for CG use.

13. Special Handling Designation (SHD). SHDs are the code words used following the classification to inform the receiving station that the record message requires special handling.

a. Special Category (SPECAT). SPECAT is a designation applied to classified record messages identified with specific projects requiring special handling procedures supplemental to those required by the security classification. The special handling procedures ensure that the record message will be handled and viewed by properly cleared personnel only. The following are specific types of SPECAT record messages:

(1) Record messages identified as Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI);

(2) Record messages identified as EXCLUSIVE FOR; and

(3) Record messages identified by the use of a code word.

b. Special Category (SPECAT) Categories. SPECAT record messages are divided into two categories: SPECAT A (SIOP-ESI) and SPECAT B (less SIOP-ESI). Control of SPECAT record messages during electronic transmission is accomplished through assignment of SHDs.

(1) SPECAT A (SIOP-ESI) record messages must be classified Top Secret.

(2) SPECAT B (less SIOP-ESI) record messages are classified according to content and shall be assigned a minimum classification of Confidential.

c. Special Category (SPECAT) EXCLUSIVE FOR (SEF). SEF is used for highly sensitive matters, high level policy, or politically sensitive information where distribution must be limited to the named recipient only. The following restrictions apply:

(1) Reserved for use by flag/general officers and officers in command status;

(2) Not intended for use in operational matters;

(3) Not to be referenced in other General Service (GENSER), narrative record messages; and

(4) Not to be readdressed. If forwarding is necessary use quote procedures.

d. PERSONAL FOR. PERSONAL FOR is the marking applied when record message distribution must be limited to the named recipient (who may, upon receipt, direct further distribution). Only flag officers, officers in command status, or their specifically designated representatives may originate PERSONAL FOR record messages. The PERSONAL FOR label shall only be applied to highly sensitive record messages that are intended for direct delivery to a flag officer or flag officer equivalent civilian official.

(1) Record messages shall not contain SSICs, passing instructions, office codes, or other record message dissemination keys.

(2) PERSONAL FOR record messages shall not be readdressed.

14. Speed of Service Objective (SOSO). SOSOs are an established set of "writer-to-reader" record message delivery time frames. These time frames are determined by the precedence assigned to a record message (see Appendix B, section B.3 for discussion of precedence). "Writer-to-reader" has traditionally been defined as the moment a record message is released into the record message system to the actual time the intended reader is viewing the record message. Continuous upgrading/improvements to CGMS have essentially automated the "writer-to-reader architecture" such that there is no longer the reliance on telecommunication personnel for record message processing. As such, the delivery emphasis has shifted from the actual person viewing the record message to the final delivery to the intended reader's record message folder. However, certain roles and responsibilities of the drafter, originator, and addressee remain.

a. Drafter/Originator Responsibilities. Traditionally, a significant amount of high precedence record messages sent through telecommunication networks (normally immediate) have failed to meet the current criteria for expeditious delivery for a variety of reasons. Additionally, record message drafters tend to believe that if they increase the precedence, it will be delivered faster or get through delivery delays at record message service facilities. These actions by the drafting/originating unit only serve to cause record message delays or backlogs and are not authorized. Commanding officers are ultimately responsible for assigning the appropriate precedence before releasing record messages and shall ensure the guidelines set forth in this Manual are strictly enforced. Commanding officers shall also carefully determine the need to send each record message regardless of precedence if the information can be passed quickly and efficiently via other appropriate means such as secure telephone, E-mail, operational voice circuits, etc.

(1) The action addressee(s) of a high precedence record message shall be notified in advance if a response is time critical. Many situations arise

which may render such notification by originators unfeasible. An example would be a flash or immediate precedence Commandant or flag level time-sensitive operational tasking record message sent to a large collective group of units. In such events, the originator should promptly notify the headquarters or appropriate area CC for assistance.

(2) If, for some reason, a record message is not delivered, follow the tracer procedures in this Manual.

b. Addressee Responsibilities. Although SOSOs are currently factored in to record message system performance with final delivery to the unit record message folder, action addressees still bear some responsibility as outlined below and commensurate with the type of unit and personnel available:

(1) Addressees with continuous watch capabilities (e.g., CCs) shall ensure that record message systems are routinely checked for receipt of high precedence record messages;

(2) Units holding record message guards for other units or detachments shall maintain appropriate oversight of all unit folders as operations dictate; and

(3) Addressees without continuous watch capabilities shall ensure effective after-hours notification methods are in place to ensure response to record messages requiring immediate action.

c. Area-Wide Communication Center (AWC) Responsibilities. Each area CAMS is responsible for meeting SOSO.

(1) AWCs shall monitor their record message systems for performance and potential backlogs.

(2) AWCs shall assist units with record message delivery problems.

15. Tracer Action. A tracer action enables the AWC to trace a record message's transmission path to determine the point at which a delay or failure occurred and corrective action to be taken. Procedures for the initiation of tracer actions are as follows and can also be found in Allied Telecommunications Record System (ALTERS) Operating Procedures, ACP 128 (series).

a. Originator/Addressee Responsibilities. If the unit suspects a record message delivery problem, the unit shall notify their CAMS via message if possible. Exhibits 10-2, 10-3, and 10-4 provides sample messages advising of delay or non-delivery of a message. Deployed cutters serviced by a NCTAMS shall notify that unit as per that unit's published procedures.

Exhibit 10-2
Record Message Delay or Non-Delivery
Notification Sample from Originator

P 101500Z JAN 12
FM CCGDFIVE PORTSMOUTH VA
TO COGARD CAMSLANT CHESAPEAKE VA
BT UNCLAS //N02310//
SUBJ: TRACER ACTIONA. MY 091200Z JAN 12
1. CCGDSEVENTEEN JUNEAU AK CLAIMS (NON-RECEIPT/DELAY) OF REF A. REQUEST INVESTIGATE AND DETERMINE THE CAUSE.
2. REQUEST ADVISE.
BT

Exhibit 10-3
Record Message Delay Notification
Sample from Addressee

P 101500Z JAN 12
FM CCGDFOURTEEN HONOLULU HI
TO COGARD CAMSPAC PT REYES CA
BT
UNCLAS //N02310//
SUBJ: TRACER ACTION
A. COMDT COGARD WASHINGTON DC 091200Z JAN 12
1. THIS UNIT EXPERIENCED INORDINATE DELAY OF REF A. REQUEST INVESTIGATE AND DETERMINE THE CAUSE.
2. REQUEST ADVISE.
BT

Exhibit 10-4
Non-Delivered Notification
Sample from Addressee

P 101500Z JAN 12
FM CCGDFOURTEEN HONOLULU HI
TO COGARD CAMSPAC PT REYES CA
BT
UNCLAS //N02310//
SUBJ: TRACER ACTION
A. PHONECON BTWN LT B.C. DELTA, D14 (DT) AND LCDR C.B. ALPHA, COMDT (CG-652) OF 10 JAN 12
B. COMDT COGARD WASHINGTON DC 091200Z JAN 12
1. PER REF A, THIS UNIT IN NON-RECEIPT OF REF B. REQUEST INVESTIGATE AND DETERMINE THE CAUSE.
2. REQUEST ADVISE.
BT

b. Area-Wide Communication Center (AWC) Responsibilities.

(1) If an originator claims a record message delay or non-delivery, the servicing AWC retransmits the record message (for non-delivery claim), examines local records to determine the cause of the delay/non-delivery, and reports back to the originator.

(2) If an addressee claims a record message delay or non-delivery, the servicing AWC retransmits the record message (for non-delivery claim), the servicing AWC examines local records, audit trails, and logs to determine if the record message is locally held, and advises the addressee accordingly.

(3) Should local checks reveal that the delay or non-delivery occurred outside of AWC assets, the AWC shall initiate appropriate tracer action and advise accordingly.

16. High-Precedence Record Message System Testing. Areas are tasked with determining record message system performance and unit notification capabilities and shall conduct high-precedence record message system testing (flash precedence only). Determine high-precedence testing results by the time a test record message actually populates the addressee's record message folders rather than the time-of-receipt (TOR) of the record message's response. The record message's action addressees shall notify the area office via the quickest means available.

a. Areas shall conduct high-precedence tests quarterly, alternating between classified and unclassified record message systems.

b. Areas shall select twelve random units, with emphasis on providing a good cross-section of unit types under varying operational status within AORs, e.g., at least one each underway cutter, cutter moored away from homeport (if applicable), cutter moored homeport, area unit, district, sector, units without communication watch personnel, etc.

c. Areas shall track results of high-precedence tests, capturing the following information:

(1) Test record message date-time-group (DTG);

(2) Addressees;

(3) Addressees' operational status (if applicable);

(4) Times of record message folder delivery and time of notification that the record message was acknowledged by the addressees;

(5) Reasons SOSO was not met, if applicable; and

(6) Other problems identified by the test.

d. Test results shall be retained for 1 year.

17. Message Text. All CG generated record messages shall be drafted in upper case letters only. Most record messaging systems currently in use within the CG and DOD are able to process upper and lower case characters. However, there is still limited use of systems which can only handle upper case.

18. Allowable Characters. Characters authorized for use in record messages (all types) appear in Exhibit 10-4.

Exhibit 10-4
Authorized Characters for Record Messages

Character	Definition
“	Quotation mark
.	Period
,	Comma
:	Colon
( )	Parentheses
?	Question mark
-	Hyphen
/	Slant
Alphabetic characters (A through Z (capitalized letters)) Numeric’s (0 through 9) Blank spaces The character @ shall be rendered as (AT), e.g., Name(AT)uscg.mil	

19. Record Message Cancellations.

a. Only originators may cancel record messages.

b. Record messages are cancelled by a new properly prepared and released record message.

c. Record messages shall be cancelled only with a cancellation record message or within the text of a new record message. A cancellation record message will reference the original record message and include a brief statement to explain the action being taken (e.g., MESSAGE SENT IN ERROR. CORRECTION TO FOLLOW). The cancellation record message subject line is the same as the original record message. If cancelling a record message within the text of a new record message, the original record message shall be listed as the first reference and the first paragraph shall state “CANCEL REF A”.

20. Record Message Corrections. In the event the originator needs to change the text of a message after it has been transmitted, this can be accomplished by means of a new message containing corrections to the original message. If changes are

substantial, the originator should consider cancelling the original message and originating a new message.

21. Canned Record Messages. Canned record messages refer to locally generated PROFORMA record messages. Drafters must exercise caution to ensure record message content is up-to-date as these types of record messages could be a major source of record message corrections and retransmissions.

22. Acknowledgements. Originators may request an acknowledgement of receipt by the addressees by placing "ACKNOWLEDGE" as the last word of the text (in its own paragraph) in a modified ACP 126 (series) formatted (i.e., non-General Administrative (GENADMIN)) message. If using GENADMIN formatted messages, use an optional set, "AKNLDG/", for this purpose. Refer to the Telecommunications Users Manual, NTP 3 (series), Appendix A, for guidance.

    a. When an acknowledgement is requested, it is the responsibility of the action officer to prepare the acknowledgement.

    b. The acknowledgement shall consist of the PLA of the originator and the DTG of the message requiring acknowledgement, followed by the word "ACKNOWLEDGED."

    c. Acknowledgements shall be addressed only to the originator of the record message requiring acknowledgement.

    d. Both classified and unclassified record messages may be acknowledged in this manner.

    e. An acknowledgement indicates that a record message has been received and understood.

    f. If a prompt reply is made to a record message requiring acknowledgement a separate acknowledgement is not required.

23. Readdressals.

    a. When it becomes necessary to readdress a record message to addressees not included on the original record message, readdressals shall be restricted to the intended new recipient to preclude record messages being duplicated.

    b. The originator or an action addressee may readdress a record message to another addressee for action (TO) or information (INFO). An information addressee may readdress a record message only for INFO.

    c. The precedence of the readdressal may be equal to or lower than that of the original record message. In the case of a dual precedence record message, an INFO addressee may readdress the record message for INFO at or below the INFO precedence of the original record message.

d. It is not required to inform the originator and addressees of the original record message of a record message readdressal. However, if an addressee finds it necessary to repeatedly readdress recurrent record messages, the originator of these record messages should be contacted and requested to include the readdressal addressees in future record messages.

e. Exhibit 10-5 shows an example of a readdressal.

Exhibit 10-5
Record Message Readdressal Example

R 151500Z JAN 12
FM COMLANTAREA COGARD PORTSMOUTH VA//LANT-6//
TO COGARD CAMSLANT CHESAPEAKE VA
INFO COMDT COGARD WASHINGTON DC//CG-652//
P 141500Z JAN 12
FM USCGC DALLAS
TO COMLANTAREA COGARD PORTSMOUTH VA//LANT-6//
BT
UNCLAS //N02310//
SUBJ: EXAMPLE OF A MESSAGE READDRESSAL
A. TELECOMMUNICATION MANUAL, COMDTINST M2000.3 (SERIES), CHAPTER 10
1. THIS IS AN EXAMPLE OF A MESSAGE READDRESSAL.
2. THE ORIGINATOR OR AN ACTION ADDRESSEE OF THE MESSAGE TO BE READDRESSED MAY READDRESS TO ACTION AND/OR INFORMATION ADDRESSEES.
3. AN INFORMATION ADDRESSEE OF THE MESSAGE TO BE READDRESSED MAY READDRESS TO INFORMATION ADDRESSEES ONLY.
BT

24. Quoting Record Messages. Quoted record messages are sent in the event that the entire content of a record message needs to be included within a new record message. Examples include SPECAT EXCLUSIVE FOR and PERSONAL FOR record messages which may not be readdressed as outlined above. Exhibit 10-6 shows an example of a quoted record message.

Exhibit 10-6
Quoted Message Example

CLASSIFIED FOR ILLUSTRATION PURPOSES ONLY
R 161500Z JAN 12
FM COMDT COGARD WASHINGTON DC//CG-6//
TO COMPACAREA COGARD ALAMEDA CA//P//
BT
S E C R E T SPECAT EXCLUSIVE FOR (NAME) //N02319//
(REFERENCES, COMMENTS, ETC.)
QUOTE
R 150900Z JAN 12
FM COMPACFLT
TO COMDT COGARD WASHINGTON DC
BT
S E C R E T SPECAT EXCLUSIVE FOR (NAME) //N02319//
(TEXT)
BT
UNQUOTE
BT

C. Retention of Record Messages. A copy of each record message shall be retained at the CAMS for 90 days. Units requiring a copy of a record message over 90 days old must contact the originator. The following exceptions apply:

1. CG Originated Record Messages. The originating office shall retain a copy (paper or electronic) for 90 days or until the information contained therein is no longer effective.

2. Record Messages Addressed to an Action Office. The action office shall retain a copy (paper or electronic) for 90 days or until the information contained therein is no longer effective.

3. General Record Messages. A copy of each CG/ DOD/ Department of the Navy (DON) generated general record messages shall be maintained by the CAMS until cancelled by the promulgating authority.

4. CAD Promulgation, Modification, or Recapitulation Record Messages. A copy of each CG generated CAD promulgation, modification, or recapitulation record message, and all those generated by DOD/DON guarded by the CG, shall be maintained by the CAMS until cancelled by the promulgating authority.

5. AIG Promulgation, Modification, or Recapitulation Record Messages. A copy of each CG generated AIG promulgation, modification, or recapitulation record message including specific DOD/DON generated AIGs that the CG requires, shall be maintained by the CAMS until cancelled by the promulgating authority.

6. Record Message Tracer File. Retain tracers for 6 months following resolution.

7. High-Precedence Message Test Results. Retain for 1 year.

D. Record Message Delivery for Underway Units. Servicing CAMS or NCTAMS deliver record messages to underway units using the systems listed in Exhibit 10-7.

Exhibit 10-7
Record Message Delivery Methods for Underway CG Cutters

	Fleet SIPRNET Messaging (FSM)	Common User Digital Information Exchange (CUDIXS)	Coast Guard Fleet SIPRNET Messaging (CGFSM)	Secure Data Exchange (SDX)	High Frequency Data Exchange (HFDX)	Fleet Broadcast
WMSL (421')	(P)	S (Note 2)	P			T (Note 2)
WAGB (420')		S		P		T
WAGB (399')	P	S				T
WHEC (378')	P	S (Note 2)				T (Note 2)
WIX (327') - NIPR Only			P			
WMEC (282')			P	S	T (Note 3)	
WMEC (270')	P	S (Note 2)				T (Note 2)
WLBB (240')				P		
WLB (225')			P	S		
WMEC (210')			P	S		
WLM (175')**						
WLIC (160')**						
WTGB (140')				P		
WPB (110') - PATFORSWA*			P	S		
WPB (110') - NON-PATFORSWA				P		
WLIC (100')**						
WLI (100')**						
WPB (87')**						

P: primary; S: secondary; T: tertiary; (P): primary when installed
*PATFORSWA (Patrol Forces Southwest Asia)
** Record messages received via voice, as necessary
Note 1: Voice comms for message traffic is the primary path if all data comms are inoperative.
Note 2: For Top Secret messaging, CUDIXS is primary and fleet broadcast is secondary.
Note 3: HFDX primary if CGFSM/SDX not reliable (Arctic Region).

E. Electronic Mail (E-mail). As per The Coast Guard Correspondence Manual, COMDTINST M5216.4 (series), E-mail may be used to transmit official correspondence and constitutes an agency record.

1. Organizational Electronic Mail (E-mail). Organizational E-mail is defined in Management of Electronic Mail, COMDTINST 5270.1 (series) as E-mail between organizational elements that requires approval by officials with signature authority. Such correspondence must be released by command authority and should be sent with a return receipt requested to verify that delivery occurred. As specified in the Department of Homeland Security (DHS) Management Directive 11042, "FOUO information transmitted via email should be protected by encryption or transmitted within secure communications systems." Furthermore, "Recipients of FOUO information will comply with any email restrictions imposed by the originator." The CGOne network meets requirements for encryption of FOUO information. However, official CG E-mail and record

messages shall not be auto-forwarded outside the protected environment of CGOne.

2. Personal Use of E-Mail. Specific guidance on the personal use of E-mail can be found in Limited Personal Use of Government Office Equipment and Services, COMDTINST 5375.1 (series).

F. 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. Unlike E-mail, anyone with access to the chat room (which may be restricted to specific participants) can follow the thread as far back as necessary without having to be an addressee.

1. Area, district commanders and commanding officers shall specify requirements for operational employment of chat in their Annex K to Area OPLAN, OPTASK Communications or unit SOPs.

2. When directed by Annex K to Area OPLAN, OPTASK, or SOP, chat sessions shall be recorded and saved as a communications log per Chapter 6 of this Manual.

   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.

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

3. Specific guidance on the personal use of chat can be found in Limited Personal Use of Government Office Equipment, COMDTINST 5375.1(series).

G. 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 may be used for operational purposes under the following circumstances:

1. Area, district commanders and commanding officers shall specify requirements 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 shall be recorded (manually if necessary) and saved as a communications log per Chapter 6 of this Manual.

CHAPTER 11 DISTRESS, SEARCH AND RESCUE (SAR), AND MEDICO COMMUNICATION

A. Mission.

1. General. One of the primary functions performed by CG telecommunication personnel is to provide rapid and reliable communication to vessels in distress.

   a. Under 14 U.S.C 2 § 2 the CG shall 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 United States covering all matters not specifically delegated by law to some other executive department.

   b. CG personnel involved with SAR responsibilities shall adhere to current procedures described in the 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), Communications Instructions Distress and Rescue Procedures, ACP 135 (series), and ITU Radio Regulations.

2. Importance and Mission of Search and Rescue (SAR) Telecommunication. The objective of SAR telecommunication 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. Telecommunication procedures relative to distress and those pertaining to the use of the distress, urgency, and safety signals are contained in articles 30 through 34 of the 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 the 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).

2. Coordination of Search and Rescue (SAR) Telecommunication. The coordination of telecommunication relating to SAR incidents closely follows the command structure of the SAR case.

   a. The SAR mission coordinator (SMC) coordinates and manages the overall response to a SAR incident, thus is responsible for maintaining oversight of all telecommunication related to the SAR.

   b. The on-scene coordinator reports to the operational commander and is subject to tasking by the SMC. The on-scene coordinator must have rapid and

reliable telecommunications to execute command and control decisions given by the SMC.

c. The Search and Rescue Unit (SRU), defined as all assets on scene in support of a SAR incident, is subordinate to and tasked by the SMC via the on-scene coordinator. All communications destined for the SMC shall be via the on-scene coordinator.

3. Distress Communication Responsibilities. Area and district commanders shall organize the communication facilities in their AOR, and shall provide detailed instructions for the correct procedure for reporting and broadcasting distress information. These facilities provide the distress communication services listed below.

a. Continuous radio watches on distress frequencies by as many units as necessary to provide adequate coverage. All units shall proactively respond to all distress calls received and ensure they are relayed to the appropriate CC/RCC. Specific frequency guard requirements for shore facilities are listed in Chapter 12 of this Manual and frequency guard requirements for cutters are in Chapter 8 of this Manual.

b. Prompt broadcast of distress information, per current laws and privacy policies, to the maritime public which 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 shall not be released for publication.

(2) Public requests for the release of recorded audio or logs shall be referred to the unit's Freedom of Information Act (FOIA) coordinator.

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 shall immediately cease transmission and continue to listen on the frequency used for the transmission of the distress until satisfied that assistance is being rendered. No transmissions are allowed to interfere with distress traffic.

b. A distress call is not addressed to a particular station and acknowledgment of receipt shall not be given until the distress call is completed.

2. Medical Communication (MEDICO). International Radio Medical Center (CIRM) was established in 1935 in Rome, Italy, to provide, via radio, free assistance and medical advice to seamen from all over the world. MEDICOs and Medical Evacuations (MEDEVAC) are part of the traditional CG SAR mission and the CG provides message relay services for CIRM. NGA's Radio Navigational Aids, Pub 117 (series) and ITU's "List of Radiodetermination and Special Service Stations" lists commercial and government radio stations providing free medical message services to ships. Distress messages of this nature should be prefixed DH MEDICO.

   a. The CG accepts DH MEDICO messages and shall deliver them to the appropriate area or district CC.

   b. The CG shall deliver messages requesting medical advice to hospitals or other facilities where authorities or the communication facility involved has made prior arrangements. A qualified doctor provides the CG with the medical advice to be transmitted. RCCs and SCCs shall establish procedures for consults with medical facilities or CG assigned Public Health Service medical doctors.

   c. DH MEDICO messages received and addressed to CIRM ROMA shall be sent to either the LANTAREA or PACAREA CC for proper handling. The contact information for CIRM ROMA is as follows:

      (1) TELEX: 612068 C.I.R.M. I

      (2) Telephone: [+39] 06 54223045

      (3) Mobile GSM Telephone: [+39] 348 3984229

      (4) FAX: [+39] 06 5923333

      (5) E mail: telesoccorso@cirm.it

   d. The CG is not acting as a government agency responsible for providing free medical message service, but rather offers its radio facilities free of charge in the same manner as commercial facilities for this type of service.

   e. In some cases DH MEDICO messages sent via commercial stations are incorrectly addressed to the CG. In such cases the message shall be forwarded immediately to the appropriate area CC. Area CCs shall have local procedures in place for handling incorrectly addressed DH MEDICO messages.

   f. In the event a medical case develops a need for CG assistance, the messages shall be handled via CG units when possible. In most cases, the CG shall 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 cognizant CG officer

may send a DH MEDICO message chargeable to the CG via commercial facilities.

g. All MEDICO messages are a potential assistance case and of interest to the CG. Liaison shall be maintained with commercial facilities to attempt to ensure the CG is kept well informed of all MEDICO messages not handled via CG circuits.

3. Initial Search and Rescue (SAR) Check Sheet. Communications watchstanders shall use an initial SAR check sheet when documenting information on distress cases. An example of an Initial SAR Check Sheet is contained in Appendix G of USCG Addendum to the US National Search and Rescue Supplement (NSS) to the International and Aeronautical and Maritime Search and Rescue (IAMSAR) Manual, COMDTINST M16130.2 (series).

4. Distress, Emergency, and Safety System Frequencies. Telecommunication personnel may receive a distress call or message in a variety of forms. A complete list of these systems and their associated frequencies appear in Chapter 12 of this Manual.

5. Distress Electronic Mail (E-mail) and Text Messaging Policy. Some communication providers offer E-mail and text messaging capabilities. E-mail and text messaging are not designed for distress communication, and the CG does not endorse their use for distress alerting purposes. Additional information regarding distress e-mail and text messaging is contained in USCG Addendum to the US National Search and Rescue Supplement (NSS) to the International and Aeronautical and Maritime Search and Rescue (IAMSAR) Manual, COMDTINST M16130.2 (series).

6. Telephone Policy. The commanding officer or officer-in-charge of each unit shall ensure personnel are proficient in handling telephone calls, particularly those of a distress nature, terrorist threat, or bomb threat, before assigning them to duty answering telephones. In addition, if the CG unit cannot take action in response to a distress call, terrorist threat, or bomb threat, the commanding officer or officer-in-charge shall ensure personnel know how to relay the information to appropriate supervisors or authorities.

7. Distress Cellular Telephone Policy. Cellular telephone usage, in the maritime community, has grown rapidly, and an increasing number of boaters are relying on cellular telephones in conjunction with, or sometimes instead of, VHF-FM radio. Cellular telephones are not considered a replacement for VHF-FM radio.

a. When properly used, as per the USCG Addendum to the US National Search and Rescue Supplement (NSS) to the International and Aeronautical and Maritime Search and Rescue (IAMSAR) Manual, COMDTINST M16130.2 (series), cellular phones meet the requirements of reliable communication.

b. When a distress call is received via cell phone and the caller's location is not known, use the procedures in Exhibit 11-1 to determine the location of the caller.

Exhibit 11-1
Cellular Tower Location Procedure

Step	Action
1	Obtain the caller's name, cellular number, and cellular provider.
2	If unable to obtain the provider from the caller, enter the cellular number into http://www.fonefinder.net/ to determine the provider.
3	Contact the provider's Subpoena/Court Order Compliance Center and request the tower location (and height) for the most recent call. SPRINT/NEXTEL: (888) 877-7330 AT&T: (800) 635-6840 VERIZON: (800) 451-5242 US CELLULAR: (630) 875-8270 or (865)777-8200 (after hours)
4	Explain that you are from a CG emergency response center, and you have received or are the intended recipient of a distress call from a cellular phone serviced by the provider per 18 U.S.C. 2702(b)(1) & (3). **If applicable, tell the provider's center that you have determined that an emergency exists that involves immediate danger of death or serious physical injury, and that per 18 U.S.C. 2702(b)(8) this emergency justifies disclosure of cell tower information without delay.**

D. Medium Frequency (MF) Communication Policy. 2182 kHz is the international MF distress and calling frequency. As such, the CG requires commercial fishing vessels, and the FCC requires small passenger vessels, to carry MF transceivers to communicate with the CG in the event of a distress or other emergency. The CG broadcasts urgent marine information broadcasts (UMIB), BNMs, and weather warnings on 2670 kHz for vessels outside VHF range.

1. CAMS, COMMSTA Kodiak and all SCCs (except those in CG District 9) are required to maintain an effective 24/7 communications watch on single sideband MF frequency 2182 kHz. Specific area requirements are outlined in Annex K to Area OPLAN.

2. 2182 kHz monitoring requirements for CG vessels are listed in Chapter 12 of this Manual.

3. 2182 kHz system performance shall be checked and verified every 8 hours. Receiver squelch/volume controls shall be set and maintained at sufficient audio level(s) to provide an effective continuous communications watch.

4. Broadcast of UMIBs, BNMs and weather, per Chapter 13 of this Manual, shall be made on 2670 kHz after initial broadcast announcement on 2182 kHz.

5. CASREPs shall be submitted immediately in the event of equipment failure impacting the unit's 2182 kHz monitoring or 2670 kHz broadcast capabilities.

E. Very High Frequency (VHF) Communication Policy. VHF-FM systems are the preferred and most effective method of voice communication in sea area A1 (see Chapter 12 of this Manual). Within this Area, the CG operates NDRS and R21. While both provide monitoring and broadcast capabilities, R21 adds direction finding and DSC. Remaining NDRS provides coverage in isolated locations only where there is no R21 coverage.. Refer to Appendix C, R21 Operational Guidance, for specific operating procedures.

1. National Distress and Response System (NDRS) and Rescue 21 (R21) Communication System Operational Guidance. When using NDRS and R21 in tandem, watchstanders shall use all available tools from both systems to communicate with and locate a vessel in distress.

   a. If the two systems provide conflicting data that cannot be resolved, both data sets shall be used for case analysis in search planning.

   b. Until R21 at each sector is accepted and the legacy NDRS system is secured, maintain and monitor both R21 and legacy VHF-FM Channel 16 (156.800 MHz) guard capabilities to ensure coverage of the AOR.

2. Rescue 21 (R21) Direction Finding (DF) Monitoring.

   a. The primary R21 DF receiver at each R21 Remote Fixed Facility (RFF) is permanently tuned to VHF-FM Channel 16 (156.800 MHz).

   b. The secondary R21 DF receiver shall remain tuned to VHF-FM Channel 70 DSC (156.525 MHz) unless temporarily tuned to 121.5 MHz or different VHF-FM working channel to meet other operational use.

   c. Units receiving DSC distress calls, including those calls using invalid or unregistered 9-digit MMSI, shall tune their secondary R21 DF receiver to VHF-FM Channel 70 DSC (156.525 MHz) using the R21 DF Manager, DF Configuration settings.

CHAPTER 12 GLOBAL MARITIME DISTRESS AND SAFETY SYSTEM (GMDSS) AND MARITIME MOBILE SERVICE IDENTITIES (MMSI)

A. Introduction. GMDSS uses terrestrial and satellite technology and shipboard radio systems to ensure rapid, automated alerting of shore-based communication and rescue authorities, in addition to ships in the immediate vicinity, in the event of a marine distress. GMDSS was established by the IMO in 1988, and comprises the umbrella of internationally approved distress telecommunication systems. Under the GMDSS, all cargo ships 300 gross registered tons and upwards, and all passenger ships on international voyages, i.e., vessels subject to the SOLAS Convention, must be equipped with radio equipment that conforms to international standards as set out in the system. The basic concept is that search and rescue authorities ashore, as well as shipping in the immediate vicinity of the ship in distress, will be rapidly alerted through satellite and terrestrial communication techniques so that they can assist in a coordinated search and rescue operation with minimum delay. The 406 MHz Emergency Position Indicating Radio Beacon (EPIRB) is the internationally recognized method of satellite distress alerting under GMDSS. DSC is the internationally recognized method of sending a terrestrial 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. Information in this Chapter is taken directly or indirectly from ITU Radio Regulations.

1. Harmful Interference. Any emission causing harmful interference to distress and safety communication on any of the discreet GMDSS frequencies is prohibited. Before transmitting for other than distress purposes on any GMDSS frequency, a station shall, where practicable, listen on the frequency concerned to make sure that no distress transmission is being sent.

2. Test Transmissions. The number and duration of test transmissions shall be kept to a minimum on GMDSS frequencies; they should be coordinated with a competent authority, as necessary, and, whenever practicable, be carried out on artificial antennas or with reduced power. Testing on the distress and safety calling frequencies should be avoided, but where this is unavoidable, it should be indicated that these are test transmissions.

3. Survival Craft Stations. Radiotelephone equipment installed in survival craft which is capable of operating in the frequency range of 156 MHz to 174 MHz shall be able to transmit and receive on VHF-FM Channel 16 (156.800 MHz) and at least one other frequency in that range.

4. General Distress Traffic Policy. 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.

    a. For distress traffic by radiotelephony, when establishing communication, calls shall be prefixed by the distress signal MAYDAY.

b. Error correction techniques shall 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 (forward error correction (FEC)) mode. The automatic repeat request (ARQ) mode may subsequently be used when it is advantageous to do so.

c. The RCC responsible for coordinating a SAR operation shall also coordinate the distress traffic relating to the incident or may appoint another station to do so.

(1) The RCC coordinating distress traffic, the unit coordinating SAR operations, or the coast station involved may impose silence on stations which interfere with that traffic. This instruction shall be addressed to all stations or to one station only, according to circumstances. In either case, the following shall be used:

(a) In radiotelephony, the signal SEELONCE MAYDAY; and

(b) In narrow-band direct-printing telegraphy normally using FEC, the signal SILENCE MAYDAY. However, the ARQ mode may be used when it is advantageous to do so.

(2) When distress traffic has ceased on frequencies which have been used for distress traffic, the RCC controlling a SAR operation shall initiate a message for transmission on these frequencies indicating that distress traffic has finished. In radiotelephony, the message consists of the following:

(a) The distress signal MAYDAY;

(b) The call ALL STATIONS spoken three times;

(c) The words THIS IS;

(d) The call sign or other identification of the station sending the message;

(e) The date and time in UTC;

(f) The name and call sign of the vessel which was in distress; and

(g) The words SEELONCE FENEE, OUT.

d. On-scene communication is that between the vessel in distress and the assisting response units, and between the response units and the unit coordinating SAR operations. Control of on-scene communication is the responsibility of the unit coordinating SAR operations. Simplex communication shall be used so that all on-scene response units may share relevant information concerning the distress incident. If direct-printing telegraphy (i.e., SITOR), it shall be in the FEC mode.

5. General Urgency and Safety Communication. Urgency and safety communication includes navigation and meteorological warning and urgent information, ship-to-ship safety of navigation communication, ship reporting communication, support communication for SAR operations, other urgency and safety messages, and communication relating to the navigation, movements, and needs of ships and weather observation messages destined for an official meteorological service.

   a. In a terrestrial system, a preliminary announcement shall be made on calling and distress frequencies prior to urgent or safety broadcast transmission. A preliminary announcement is not required for urgent or safety broadcasts conducted via the maritime mobile satellite service.

   b. The urgency signal consists of the words 'PAN PAN' (pronounced PAHN PAHN). The signal indicates that the calling station has a very urgent message to transmit concerning the safety of a mobile unit or a person.

      (1) Medical transports are transportation by land, water, or air, whether military or civilian, permanent or temporary, assigned exclusively to medical transportation and under the control of a competent authority of a party to a conflict or of neutral States and of other States not parties to an armed conflict, when these ships, craft, and aircraft assist the wounded, the sick, and the shipwrecked.

      (2) For the purpose of announcing and identifying medical transports which are protected under the 1949 Geneva Conventions and Additional Protocols, the procedures for urgency broadcast shall be followed, with the urgency signal followed by the single word 'MEDICAL' (pronounced MAY-DEE-CAL).

   c. The safety signal consists of the word 'SECURITY' (pronounced SEECURITAY). The safety signal indicates that the calling station has an important navigational or meteorological warning to transmit.

6. Transmission of Maritime Safety Information (MSI). Messages from ship stations containing information concerning the presence of severe weather, dangerous ice, dangerous wrecks, or any other imminent danger to marine navigation, shall be transmitted, with the least possible delay, to other response units in the vicinity and to the appropriate authorities at the first point of the coast with which contact can be established. These transmissions shall be preceded by the safety signal.

   a. MSI shall be transmitted by means of narrow-band-direct-printing (NBDP) telegraphy with FEC using the frequency 518 kHz as per the international NAVTEX systems.

   b. Maritime safety information is transmitted by means of NBDP telegraphy with FEC using the frequencies 4210 kHz, 6314 kHz, 8416.5 kHz,

12579 kHz, 16806.5 kHz, 19680.5 kHz, 22376 kHz, and 26100.5 kHz (on-request only).

7. Intership Navigation Safety Communication. Intership (bridge-to-bridge) navigation safety communication is that VHF radiotelephone communication conducted between ships for the purpose of contributing to the safe movement of ships. VHF-FM Channel 13 156.650 MHz is used for intership navigation safety communication. In the Gulf of Mexico and on the Mississippi River VHF-FM Channel 67 (156.375 MHz) is also used.

8. 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 shall be capable of transmitting on the following frequencies:

   a. On the carrier frequency 2182 kHz, on the carrier frequency 4125 kHz, or on the carrier frequency VHF-FM Channel 16 (156.800 MHz).

   b. On the carrier frequency 2182 kHz or the carrier frequency 4125 kHz, on the frequency VHF-FM Channel 16 (156.800 MHz) and, optionally, VHF-FM Channel 9 (156.3 MHz).

B. 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:

1. 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. Sea area A1 will be implemented in the United States upon completion of R21 system deployment.

2. 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.

3. Sea Area A3. An area within the coverage of an Inmarsat geostationary satellite (excluding sea areas Al and A2) in which continuous alerting is available. Ships traveling this area must carry either an Inmarsat B or C 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.

4. 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 and A2.

C. Global Maritime Distress and Safety System (GMDSS) Sub-Systems. GMDSS consists of numerous telecommunication sub-systems, including:

1. Digital Selective Calling (DSC). Used for distress, urgency, safety, routine, ships business, and test calling via HF, MF, and VHF-FM.

2. Navigational Telex (NAVTEX). Narrow-band direct-printing telegraphy for transmission of navigational and meteorological warnings and urgent information to ships on MF.

3. Simplex Teletype Over Radio (SITOR). Used for ship-to-shore communication and transmissions of MSI.

4. Inmarsat B and Fleet-77. Ship-to-ship and shore-to-ship voice, telex, and fax communication utilizing satellite. These terminals can be interconnected to public switched telephone and data networks.

5. Inmarsat C. Used for distress alerting, data communication, and reception of MSI.

6. Radio Telephone. Used for transmission via MF, HF, and VHF-FM.

7. Satellite. EPIRB used for distress alerting and locating survivors of distress incidents (406 MHz).

8. Search and Rescue Transponder (SART). Used for locating survival craft.

9. Automatic Identification System-Search and Rescue Transmitter (AIS SART). SAR transmitter used for locating survival craft.

D. Maritime Mobile Service Identity (MMSI) Numbers. The IMO has adopted the ITU MMSI as an internationally recognized method mainly for identifying AIS transmissions and DSC transmissions.

1. General. MMSIs are nine digit numbers used by maritime DSC, automatic identification systems (AIS) and certain other equipment to uniquely identify a ship or a coast radio station. MMSIs are regulated and managed internationally by 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.585-5.

2. Maritime Mobile Service Identity (MMSI) Maintenance. Commandant (CG-652) is responsible for providing and registering CG MMSIs. Newly established CG shore and afloat units without an MMSI can request one from Commandant (CG-652) via official record message, telephone call, or E-mail to

russell.s.levin@uscg.mil. Commandant (CG-652) will also verify the assignment or non-assignment of any CG MMSI upon request. Acquisition activities are responsible for obtaining MMSIs for any equipment requiring one through coordination with Commandant (CG-652). NAVCEN monitors and reports incorrect AIS & Encrypted Automatic Identification System (EAIS) errors by utilizing NAIS data.

3. Maritime Mobile Service Identity (MMSI) Search and Rescue (SAR) Vessel Identification System. In response to the SAR Program requirement for accurate registration information on the owners of DSC radios, CG OSC replaced the SAR ID Database with the web-based MMSI Vessel Identification System ("MMSI Database"). The MMSI Database is a web-based application that can be accessed via CGOne at the following URL: http://misle.osc.uscg.mil/mmsi/. The link http://mislenet.osc.uscg.mil/ also contains guidance for new user access if necessary. Users granted access to the Automated Mutual Assistance Vessel Rescue (AMVER) Surface Picture (SURPIC) application will automatically be given access to the MMSI Database.

E. Digital Selective Calling (DSC). DSC is a digital technology intended to initiate non-voice communication over maritime radio and provide distress alert information to CG CCs and foreign RCC. DSC allows mariners to instantly send an automatically formatted distress alert to the CG or other rescue authority anywhere in the world. 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. DSC distress calls may be electronically relayed to the CG by any vessel that has a DSC compatible radio. Users of DSC may call a specific station, group of stations, or all stations to establish communication. DSC calls are made using the applicable MMSI number and appropriate DSC guard or calling frequencies, depending upon whether it is a distress alert or another type of call. Detailed policy for CG units equipped with DSC is provided in this section.

1. General. Units receiving DSC distress alerts should first acknowledge receipt of the call via DSC and then attempt to establish voice communication on an appropriate channel. Afloat units must wait 5 minutes to allow the shore units to respond. If there is no response then the afloat unit shall respond to the call and relay the alert to the nearest CG shore unit. CG aircraft in receipt of a DSC alert will relay the pertinent alert information to their operational commander via the most expeditious means available. CC personnel should 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. There are no restrictions on CC personnel contacting foreign RCCs for the purposes of SAR operations.

2. Digital Selective Calling (DSC) Categories. DSC calls fall into the following categories: distress, urgency, safety, and routine. The most 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.

3. General Digital Selective Calling (DSC) International Telecommunications Union (ITU) Requirements.

   a. 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 MF and VHF bands. Additionally, HF may be used.

   b. A station in the mobile or mobile-satellite service which learns of a vessel in distress shall initiate and transmit a distress alert when the vessel itself is not able to transmit the distress alert. The station transmitting a distress alert relay shall indicate that it is not in distress. Acknowledgement of a distress RELAY via radiotelephone shall be in the following format:

      (1) The distress signal MAYDAY RELAY spoken 3 times;

      (2) ALL STATIONS or coast station name, as appropriate, spoken 3 times;

      (3) The words THIS IS;

      (4) The name of the relaying station, spoken 3 times;

      (5) The call sign to include other identification (i.e. MMSI) of the relaying station that may be necessary; and

      (6) Send as completely as possible, the original distress message as received with all the necessary information.

   c. Acknowledgement by radiotelephone of RECEIPT of a distress alert from a ship station or ship earth station shall be given in the following form:

      (1) The distress signal MAYDAY;

      (2) The name followed by the call sign, or the MMSI or other identification of the station sending the distress message;

      (3) The words THIS IS;

      (4) The name and call sign or other identification of the station acknowledging receipt;

      (5) The word RECEIVED; and

      (6) The distress signal MAYDAY.

   d. Coast stations and appropriate coast earth stations in receipt of distress alerts shall ensure that they are routed as soon as possible to a RCC.

   e. Radiotelephone distress acknowledgement responsibilities for ships:

      (1) In areas where reliable communications with one or more coast stations are practical, ships in receipt of a distress alert and/or call from another

vessel should defer acknowledgement for a short interval so that a coast station may acknowledge receipt first;

(2) In areas where reliable communications are not practical and a distress alert and/or call is received is within a ship's operating vicinity, the ship shall acknowledge receipt and advise the calling vessel that their distress call is being relayed to the nearest RCC. Further action shall only be at the direction of the cognizant operational commander;

(3) Ships in receipt of distress call via VHF-FM Channel 16 (156.800 MHz) that goes unanswered for 5 minutes shall acknowledge receipt and relay as soon as possible to the nearest RCC; and

(4) To avoid unnecessary confusion or duplication when receiving a distress call/alert via HF, a ship shall listen for 5 minutes and if no response to the call is heard, the ship shall not respond but shall relay the distress information only to the appropriate coast station/RCC.

4. Digital Selective Calling (DSC) Guard Requirements.

a. Ashore.

(1) CG CAMS and COMMSTA Kodiak shall guard 6 DSC frequencies: 2187.5 kHz, 4207.5 kHz, 6312.0 kHz, 8414.5 kHz, 12577.0 kHz, and 16804.5 kHz.

(a) The DSC system will log test calls on all frequencies but filters all test calls except on 4 MHz. The 4 MHz frequency has the Automatic Test Call Answering (ATA) function enabled and will automatically respond to all tests received. The ATA is not enabled on the other MF/HF DSC frequencies but test calls can still be manually answered.

(b) HF DSC equipped units are not required to answer tests on other frequencies and are discouraged from doing so.

(2) CG sectors equipped with MF DSC shall guard 2187.5 kHz. MF DSC equipped units are not required to answer tests on other frequencies and are discouraged from doing so.

(3) CG sectors equipped with R21 shall guard VHF-FM Channel 70 (156.525 MHz). DSC test calls received via VHF will automatically be answered by the R21 system and do not require operator intervention.

b. Digital Selective Calling (DSC) Guard Frequencies. DSC guard frequencies and their equivalent voice and SITOR frequencies are listed in Exhibit 12-1.

Exhibit 12-1
Digital Selective Calling (DSC) Guard Frequencies,
Associated Voice, and SITOR Frequencies

DSC Guard Frequency	Voice Frequency	SITOR Frequency
156.525 MHz	156.800 MHz	N/A
2187.5 kHz	2182 kHz	2174.5 kHz
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

c. Afloat.

(1) CG cutters underway or at anchor equipped with VHF-FM DSC radios shall guard VHF-FM Channel 70 (156.525 MHz) (DSC). CG cutters underway or at anchor equipped with HF/MF DSC radios shall guard DSC frequency 2187.5 kHz.

(2) CG cutters 110' and larger equipped with HF/MF radios, excluding WLIC class, shall monitor 2182 kHz when underway or at anchor when not engaged in two way communication.

(3) In addition to the above frequency requirements, all cutters shall guard 4125 kHz any time they operate in the Alaskan AOR.

Note: Refer to Chapter 8 for specific frequency guard requirements.

d. 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. Designated CG shore stations will maintain a continuous watch on this frequency.

e. Coast Guard (CG) Aircraft. CG aircraft equipped with VHF-FM DSC radios shall guard DSC VHF-FM Channel 70 (156.525 MHz).

5. High Frequency/Medium Frequency (HF/MF) Digital Selective Calling (DSC) Response Policy: Coast Guard (CG) Shore Units.

a. Purpose. To provide operational shore units with policy guidance for responding to HF and MF DSC distress alerts.

b. Coordination. DSC is unique in that distress communication is initiated by digital data bursts that are widely distributed, but all follow-up communication after initial acknowledgement are typically handled by voice. ITU regulations require each unit that receives a DSC distress alert or distress

relay to send an acknowledgment. As such, it is probable that multiple sectors, along with the appropriate CAMS, will receive and acknowledge the same MF DSC distress alert. It is also possible that the same distress alert may be received on both HF and MF bands. For these reasons, it is important that CG units communicate with one another and with the default SMC to ensure role clarity during DSC case operations. Shore units receiving DSC alerts outside their AOR shall wait 5 minutes. If no other units respond, then an acknowledgement shall be sent and the appropriate follow-on actions taken. Further information regarding SMC determination, delegation and responsibilities is in the 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).

6. High Frequency/Medium Frequency (HF/MF) Digital Selective Calling (DSC) Response Policy: Coast Guard (CG) Afloat Units.

   a. Purpose. To provide CG afloat assets equipped with HF/MF DSC equipment with procedures for responding to MF DSC initiated distress alerts.

   b. Discussion. CG cutters upgraded to include the DSC capability are required to guard 2187.5 kHz (DSC), and 110' and greater cutters, excluding WLIC class, are required to monitor 2182 kHz voice when underway. Cutters equipped with DSC radios may receive a DSC distress alert on 2187.5 kHz (DSC).

   c. Action. When a DSC distress alert is received on 2187.5 kHz, the radio will emit a loud audio alarm. This alarm is the equivalent of a MAYDAY call and requires the same level of response. Cutters that receive a DSC distress alert shall take the following steps:

      (1) In areas where reliable MF DSC communications with one or more shore stations are feasible, commanding officers/officers-in-charge should defer acknowledgement so that a shore station can acknowledge receipt of a call. Any cutter receiving a call that is not acknowledged by a shore station within 5 minutes shall acknowledge the call using the procedure in section E.6.c.(3) of this Chapter;

      (2) In areas where reliable MF DSC communications with a shore station are known not to exist, cutters that receive an MF DSC call shall wait at least one minute before acknowledging receipt of the distress alert; and

      (3) Cutters acknowledging receipt of a MF DSC alert shall:

         (a) Acknowledge receipt of the alert on 2182 kHz and attempt to establish voice communications with the distressed vessel,

         (b) If unable to establish voice communications with the distressed vessel, cutters shall 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 and terminate the DSC distress call. After sending the DSC acknowledgement, try again to establish voice communications with the distressed vessel, and

(c) Cutters that acknowledge receipt of DSC distress alerts are responsible for notifying the cognizant RCC and OPCON/TACON by the most expedient means and providing relevant distress vessel information (e.g., MMSI, position, nature of distress) provided by the DSC radio.

7. Very High Frequency-Frequency Modulation (VHF-FM) Digital Selective Calling (DSC) Response Policy: Coast Guard (CG) Shore Units.

a. Purpose. To provide operational shore units with policy guidance for responding to VHF-FM DSC distress alerts.

b. Discussion. The R21 system provides CG sectors with VHF-FM DSC capability. Until the CG is equipped with this capability, notification of receipt of a VHF-FM DSC distress call may be received by sectors, foreign RCCs and from third parties (including CG cutters equipped with VHF-FM DSC).

c. System Operation. 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.

(1) When a DSC distress alert is received VHF-FM Channel 70 (156.525 MHz), most of these radios will emit a loud audio alarm and then the radio will automatically shift to VHF-FM Channel 16. If the radio does not automatically shift to VHF-FM Channel 16 (156.800 MHz) then the operator shall manually shift the radio.

(2) The distressed vessel will follow the DSC distress alert with a voice transmission on VHF-FM Channel 16 (156.800 MHz).

(3) VHF-FM DSC distress alerts shall be considered the equivalent of a MAYDAY call, and shall require the same level of response.

(4) Shore-side VHF-FM DSC alert reception infrastructure is limited in the United States.

(a) The majority of VHF-FM DSC alerts received today by CG shore stations are relayed from non-CG vessels equipped with DSC radios.

(b) After the Rescue 21 system is installed in a geographic region, VHF-FM DSC alerts will be automatically received.

8. Very High Frequency-Frequency Modulation (VHF-FM) Digital Selective Calling (DSC) Response Policy: Coast Guard (CG) Afloat Units.

   a. Purpose. To provide CG afloat units equipped with VHF-FM DSC with procedures for responding to DSC initiated distress alerts.

   b. Discussion. Some CG boats and cutters have already received the VHF-FM DSC radios. The United States will not declare sea area A-1 operational until the R21 system is fully operational. Deployments of the VHF-FM DSC radios are progressing to meet the needs of radio replacement and new cutter construction projects. 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.

   c. Action. When a DSC distress alert is received on VHF-FM Channel 70 (156.525 MHz), the radio will emit a loud audio alarm and automatically shift to VHF-FM Channel 16 (156.800 MHz). If the radio does not automatically shift then manually shift to VHF-FM Channel 16 (156.800 MHz). This alarm is the equivalent of a MAYDAY call and requires the same level of response. CG boats and cutters that receive a DSC distress alert shall:

      (1) Coast Guard (CG) Boats.

         (a) As soon as possible, inform the SMC of the contents of the distress alert;

         (b) In areas where reliable VHF-FM DSC communications with one or more shore stations are feasible, coxswains shall defer acknowledgement so that a shore station can acknowledge receipt of a call. Any boat receiving a call that is not acknowledged by a shore station within 5 minutes shall acknowledge the call using the procedure in section (d) below;

         (c) In areas where reliable VHF-FM DSC communications with one or more shore stations are known not to exist, boats that receive a VHF-FM DSC distress alert shall as soon as possible, notify the appropriate SCC and acknowledge receipt of the distress alert when instructed; and

         (d) Boats acknowledging receipt of a VHF-FM DSC alert shall:

            [1] Acknowledge receipt of the alert on VHF-FM Channel 16 (156.800 MHz) and attempt to establish communications with the distressed vessel, and

            [2] If unable to establish voice communications with the distressed vessel, boats shall 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 and terminate the DSC distress call; and

[3] Boats that acknowledge receipt of DSC distress alerts are responsible for informing the applicable SCC or RCC and OPCON/TACON (if different) by the most expedient means and providing relevant distress vessel information (e.g., MMSI, position, nature of distress) provided by the DSC radio.

(2) Coast Guard (CG) Cutters.

(a) As soon as possible, inform the CO/OINC of the contents of the distress alert;

(b) In areas where reliable VHF-FM DSC communications with one or more shore stations are feasible, CO/OINCs shall defer acknowledgement so that a shore station can acknowledge receipt of a call. Any cutter receiving a call that is not acknowledged by a shore station within 5 minutes shall acknowledge the call using the procedure in section (d) below;

(c) In areas where reliable VHF-FM DSC communications with one or more shore stations are known not to exist, cutters that receive a VHF-FM DSC distress alert shall as soon as possible acknowledge receipt of a distress alert; and

(d) Cutters acknowledging receipt of a VHF-FM DSC alert shall:

[1] Acknowledge receipt of the alert on VHF-FM Channel 16 (156.800MHz) and attempt to establish voice communications with the distressed vessel,

[2] If unable to establish voice communications with the distressed vessel, cutters shall 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 and terminate the DSC distress call. After sending the DSC acknowledgement, attempt to establish voice communications with the distressed vessel, and

[3] Cutters that acknowledge receipt of DSC distress alerts are responsible for informing the applicable SCC or RCC and OPCON/TACON (if different) by the most expedient means and providing relevant distress vessel information (e.g., MMSI, position, nature of distress) provided by the DSC radio.

9. Reporting Requirements. Areas and districts may establish their own procedures for the consolidation of this statistical data which should be included in their

Annex K to Area OPLAN /district supplements, but all inputs shall be forwarded by E-mail to cgcomms@uscg.mil no later than the tenth day of the month following the month being reported.

10. Process Improvement. All units with DSC are encouraged to provide input to Commandant (CG-534) and Commandant (CG-65) via their operational commander on any procedural problems encountered or any suggestions for improving DSC response policy.

11. False Alert Violation Reporting.

    a. General. As stated in 14 U.S.C. 88, 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, a radio violation report should be submitted as per the Spectrum Management Policy and Procedures Manual, COMDTINST M2400.1 (series) for vessels, including foreign vessels in US SAR areas of responsibility, that:

        (1) Deliberately transmit false alerts;

        (2) Inadvertently transmit a false distress alert without proper cancellation;

        (3) Fail to respond to a distress alert due to misuse or negligence;

        (4) Repeatedly transmit false alerts; and

        (5) Transmit distress alert using false identity.

    b. Foreign Ship Violations. Contact local FCC Field offices to determine whether they will handle radio violations from foreign ships. If they will, violation reports should be submitted to them. If not, violation reports should be submitted as per Spectrum Management Policy and Procedures Manual, COMDTINST M2400.1 (series).

    c. False Alert Feedback Solicitations.

        (1) When a false alert is received a message should be sent by the CG unit receiving the alert to the offending vessel to ascertain the details associated with the alert.

            (a) For recreational or other small craft that may not have record messaging capability, a mailing address should be found if possible and a letter sent in lieu of a message.

            (b) The message/letter should indicate the information is being requested to assist in sorting actual distress calls from false alerts and to help improve DSC system performance.

(c) Receipt of the message/letter by the offending vessel will help to educate the mariner on the proper use of the DSC alert and implications of false alerts.

(d) Information received should be used by the CG to identify system weaknesses. This information should be forwarded to Commandant (CG-65) and Commandant (CG-534).

(2) A sample message format is provided in Appendix C, section 3 of 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). The same text should form the basis of a false alert feedback letter.

F. Navigational Telex (NAVTEX). NAVTEX is a service specifically designed for the promulgation of MSI as a part of the GMDSS. All SOLAS-regulated ships are required to carry NAVTEX receivers. NAVTEX broadcasts are made by each CAMS, COMMSTA Kodiak, Greater Antilles Section (GANTSEC), and Marianas Section (MARSEC). NAVTEX policy is administered by the IMO's International NAVTEX Coordinating Panel.

1. In general, NAVTEX coverage extends to 200 nautical miles off the coast. Coverage charts of NAVTEX service areas are published on the CG NAVCEN internet site: http://www.navcen.uscg.gov/?pageName=NAVTEX.

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

   b. The Commander, International Ice Patrol will use this system as a means of disseminating ice bulletins and warning messages.

   c. Districts, sectors, and NAVCEN will use this system as a means of disseminating NTMs.

2. If drafting NAVTEX messages, refer to Chapter 12 of the Aids to Navigation Manual - Administration, COMDTINST M16500.7 (series), for the specific formatting necessary to ensure the message reaches the target area.

3. Make every effort to keep NAVTEX broadcasts under twenty minutes.

   Note: Although IMO limits NAVTEX broadcast duration to ten minutes, the CG is authorized a twenty minute transmit duration due to greater than normal site separation in the United States.

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

G. 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, and may be

used as an alternative to satellite communication. SITOR employs a FEC mode of data for maritime safety broadcasts and ARQ for other transmissions to minimize the effects of poor HF propagation conditions. SITOR is used to broadcast MSI including high seas forecasts, navigational area (NAVAREA) warnings, ice, and hydrographic information.

H. Inmarsat. Virtually all navigable waters (less Polar Regions) of the world are covered by Inmarsat satellites. Inmarsat has several satellite constellations in geostationary orbit which transmit to Coast Earth Stations. Coast Earth Stations link the satellites with national and international telecommunication networks. Inmarsat terminals provide telephone, data, facsimile, TELEX, E-mail, and videoconferencing capabilities. Inmarsat provides service access codes (SACs) for medical advice and medical assistance. There are currently three basic types of Inmarsat terminals that can provide distress communication.

1. Fleet-77. Commercial data/voice satellite communication to include GMDSS.

2. Inmarsat B. Commercial data/voice satellite communication to include GMDSS. Inmarsat B numbers are recognized by a nine-digit number beginning with "3."

3. Inmarsat C. 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 (PC). TELEX, E-mail, 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 Coast Earth Station for broadcast. CC personnel shall 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 MSI as a part of GMDSS. The EGC system (technically a part of the Inmarsat C system) provides an automatic, global method of broadcasting messages to all GMDSS-equipped vessels in both fixed and variable geographical areas or to predetermined groups of ships.

      (1) CG RCC/CCs shall 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 shall 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, as per the 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). 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.

(4) SafetyNET services currently include:

(a) NAVAREA IV and XII navigational warning broadcasts (originated by the NGA);

(b) NAVAREA IV, XII, and XVI meteorological forecasts and warnings (originated by the NWS);

(c) Distress alerts and search and rescue warnings (originated by the USCG); and

(d) Atlantic Ocean Ice Reports (International Ice Patrol (originated by the USCG).

I. Radiotelephone. Radiotelephone is a form of telecommunication by voice radio. It is one of the most common forms of communication between the CG and federal, state, and local authorities, and the maritime public. CG radiotelephone operators must be well trained and proficient and, as CG representatives, shall always be professional. Military radiotelephone procedures shall be as per Communication Instructions Radio Telephone Procedures, ACP 125 (series). All other radiotelephone procedures shall be as per the Radiotelephone Handbook, COMDTINST M2300.7 (series) and ITU. All radiotelephone operators must first be qualified as per the Communications Watchstander Qualification Guide, COMDTINST M16120.7 (series) prior to actual use. Radiotelephone operators must also understand that strict military procedures may not always be understood by the maritime public. For this reason, when communicating with non-military vessels or aircraft, international radio procedures may be employed as necessary to ensure transmissions are understood. The following is a list of common radiotelephone frequencies:

1. Medium Frequency (MF) Radiotelephony.

a. 2182 kHz. Designated as an international calling and distress frequency for radiotelephony. This frequency is used by ships and can be used by aircraft stations in an emergency. Sectors and COMMSTA Kodiak shall maintain a continuous guard on 2182 kHz and have the capability to respond to distress and hailing within sea area A2. CG units should be aware that shipping traffic in the vicinity of the DSC distress caller may not be able to receive this traffic.

Exhibit 11-1 lists MF/HF DSC and SITOR guard frequencies. Underway cutters 110' and greater, excluding WLIC class, shall maintain a continuous listening guard on 2182 kHz.

Note: **ITU Regulations dismisses the three minute silence period observed at the top and bottom of the hour on 2182 kHz.**

b. 2670 kHz. Designated as a working frequency between CG stations and stations of the maritime community after initial contact is established on 2182 kHz. 2670 kHz is also used for CG Marine Information Broadcasts. Sectors shall have the capability to monitor and transmit on this frequency.

2. High Frequency (HF) Radiotelephony.

a. 4125 kHz. Designated GMDSS voice frequency that has a dual role within the D17 AOR as a distress and hailing voice frequency. COMMSTA Kodiak shall maintain a continuous radio watch on 4125 kHz.

b. Cutter Monitoring. Cutters shall also monitor 4125 kHz when operating within the D17 AOR.

3. Very High Frequency (VHF) Radiotelephony.

a. Very High Frequency-Frequency Modulated (VHF-FM) Channel 16 (156.800 MHz). Designated as an international distress, safety, and calling frequency for radiotelephony for stations of the maritime mobile service when they use frequencies in the authorized bands between 156 MHz and 167 MHz.

(1) To facilitate the reception of distress calls, all transmissions on VHF-FM Channel 16 (156.800 MHz) shall be kept to a minimum, and shall not exceed one minute.

(2) Urgent traffic, safety signals, MIB's announcements, and general calling shall be transmitted where practicable on a working frequency after a preliminary announcement on VHF-FM Channel 16 (156.800 MHz). Urgent broadcasts may be sent on VHF-FM Channel 16 (156.800 MHz) without shifting to a working frequency provided the entire broadcast can be sent within 1 minute.

(3) Aircraft stations may use this frequency for safety purposes only, but keep its use to a minimum, and keep transmissions under one minute duration. Refer to Chapter 9 of this Manual for additional policy.

(4) Underway cutters shall maintain a continuous listening guard on VHF-FM Channel 16 (156.800 MHz).

(5) Each SCC should include this broadcast with their regular MIB: VHF-FM Channel 16 (156.800 MHz) is for hailing and distress only, VHF-FM Channel 9 (156.45 MHz) can be used for general purpose calling.

b. Very High Frequency-Frequency Modulated (VHF-FM) Channel 9 (156.45 MHz). The increasing volume of radio calls, primarily between recreational vessels, has exceeded the capacity of VHF-FM Channel 16 (156.8 MHz). VHF-FM Channel 9 (156.45 MHz) may be used by recreational vessels for general purpose calling. This frequency should be used whenever possible to relieve congestion on channel 16. Safety and distress broadcasts will continue to be announced on VHF-FM Channel 16 (156.800 MHz). CG units equipped with R21 equipment may have to use a local radio because VHF-FM Channel 9 (156.45 MHz) is not pre-programmed into the radio.

c. VHF-FM Channel 22A (157.1 MHz). Designated as a working frequency between CG stations and stations of the maritime community after initial contact is established on VHF-FM Channel 16 (156.800 MHz). VHF-FM Channel 22A (157.1 MHz) is also used for CG MIBs.

d. 121.5 MHz and 123.1MHz. The aeronautical emergency frequency 121.5 MHz is used for the purposes of distress and urgency for radiotelephony by stations of the aeronautical mobile service. The aeronautical AUX frequency 123.1 MHz which is AUX to 121.5 MHz is for use by stations of the aeronautical mobile service and by other mobile and land stations engaged in coordinated search and rescue operations. Passenger ships subject to the SOLAS Convention are required to have means for two-way on-scene radio communications for SAR purposes using the frequencies 121.5 MHz and 123.1 MHz.

e. 243.0 MHz. The aeronautical emergency frequency 243.0 MHz is designated as an international survival craft and United States military common emergency frequency used to provide rescue communication between aircraft, manned space vehicles, ground stations, or surface craft experiencing an actual emergency. Aircraft and survival craft may use this frequency for EPIRBs and to broadcast urgent or safety messages. Testing of equipment on 243.0 MHz and 121.5 MHz should be coordinated with competent authorities and done only during the first 5 minutes of each hour.

J. Emergency Position-Indicating Radio Beacon (EPIRB) Emergency Locator Transmitter (ELT), and Personal Locator Beacon (PLB). EPIRBs are 406 MHz distress beacons and designed to transmit an alerting and locating signal when activated, usually by floating free when a vessel goes below the surface of the water, using 406 MHz. EPIRBs are maritime devices and as such are required to be waterproof, corrosion resistant, and able to float upright on their own (for those designed to float). EPIRBs are designed to be used in water, and actually the use of water maximizes the signal strength from the EPIRB. Aircraft on international flights are required to carry the 406 MHz distress beacon as their ELT but national regulation may allow 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 Federal Aviation Administration (FAA) regulations. PLBs are 406 MHz distress beacons used in the maritime community, as well as ashore, and can be automatically activated.

1. 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 United States, 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.

2. Emergency Position-Indicating Radio Beacon (EPIRB) Classes. The following is a list of EPIRBs that can be used by mariners and aircraft:

   a. 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; and

   b. Category II – 406/121.5 MHz Homing Signal. Similar to Category I, but manually activated. Some models are also water activated.

3. Emergency Position-Indicating Radio Beacon (EPIRB) Signals. 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.

4. Terminating False Emergency Position-Indicating Radio Beacon (EPIRB) Signals. Under the provisions set forth in 14 U.S.C. 88, the CG, in performing its maritime SAR mission, may perform any and all acts necessary to rescue and aid persons and protect and save property. This is interpreted as providing authority for the CG to terminate the accidental transmission of an EPIRB when such transmissions might interfere with signals from vessels or aircraft in actual distress.

   a. When sufficient effort has been made to determine that an EPIRB/ELT signal is being broadcast from a marine craft or aircraft which is not in a state of distress or emergency, operational commanders should take the necessary steps to have the signal turned off.

      (1) Commands shall coordinate with other agencies, particularly the FCC, to locate and silence the offending signal. If the nearest FCC field office cannot be contacted, the FCC Headquarters watch officer can be reached at (202) 418-1122.

      (2) All CG and CG AUX units should make every effort to encourage beacon users to register their beacon. Registration can be done online at www.beaconregistration.noaa.gov.

b. Signals may be turned off by the following procedures listed in their order of preference:

(1) Communicate to the operator that their EPIRB is transmitting and request they turn it off. In cases of noncompliance, warn the operator that it is a violation of federal regulations to knowingly continue to transmit, and that it could be creating a hazard to public safety;

(2) The EPIRB can be turned off if accessible without having to break into any compartment. The boarding officer can deactivate the signal by following the instructions on the device; and

(3) The district commander exercising operational control may consider further efforts to terminate the transmission if the procedures discussed in (1) and (2) are not successful.

c. Following a false EPIRB signal incident:

(1) In the event that forcible entry was directed by the district commander under section J.4.b. (3) of this chapter, appropriate steps shall be taken to safeguard the property entered and to notify the owner; and

(2) A violation report shall be submitted as per Spectrum Management Policy and Procedures Manual, COMDTINST M2400.1 (series) for all cases of false distress (e.g., EPIRB activation) by the district commander for the geographic area in which the vessel is registered, and an administrative letter shall be sent to the owner expressing concern from a SAR and safety perspective.

K. Radar Search and Rescue Transponder (SART). The radar SART, operating in the 9200-9500 MHz frequency band, is a transponder used for locating survival craft. The AIS SART discussed in section L of this Chapter may be used in lieu of the SART.

1. The SART signal appears as a distinctive line of 12 equally spaced blips (dots) on a radar screen extending outward from the SART position along its line of bearing.

2. Unique signals (swept frequency) are generated for interpretation only after being triggered by 9 GHz ship or aircraft radar.

3. Range of air is 40 nautical miles; surface is 10 nautical miles.

4. An audible alarm or light is activated on the SART when a rescue ship or aircraft is within close range.

5. Battery capacity should be at least 96 hours.

L. Automatic Identification System (AIS) Search and Rescue Transmitter (SART). The AIS SART may be used in lieu of the SART. It is used for locating survival craft by transmitting messages recognized 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 receiver (e.g., global positioning system (GPS) and updated at a rate of every minute. The AIS SART operates on VHF-FM Channel 87B (161.975 MHz) and VHF-FM 88B (162.025 MHz).

1. The AIS-SART message indicates the position, static and safety information of the unit in distress.

2. The AIS-SARTs should be detectable at a range of 5 nautical miles over water.

3. The AIS-SART should continue transmission even if the position and time synchronization from the positioning system is lost or fails.

4. The AIS-SART should transmit within 1 minute of activation.

5. Battery capacity should be at least 96 hours.

CHAPTER 13 MARINE INFORMATION BROADCASTS (MIB)

A. Policy. The CG transmits distress, urgent, and safety messages as required and makes regularly scheduled MIBs. The United States CG-National Weather Service Coordination-Liaison Working Group (UNCLOG) shall be responsible for the configuration management of NOAA's NWS text and graphic products to be broadcast by CG telecommunication facilities. In general, these transmissions shall include information vital to the maritime community operating in or approaching the coastal waters of the United States, including Alaska, Hawaii, Guam, and the Caribbean. Message formatting requirements for BNM of any type are included in the Aids to Navigation Manual - Administration, COMDTINST M16500.7 (series). Stations designated to make regularly scheduled weather broadcasts and warnings, and the applicable weather products, are listed at this web site: http://cgweb.rss.uscg.mil/communicationsportal/content/HQ_GMF/unclog.aspx.

1. Vessels Subject to the Safety of Life at Sea (SOLAS) Convention. SOLAS vessels no longer stand an open speaker watch on MF/HF and only respond to DSC calls. Therefore, the following policy shall apply when conducting the broadcasts specified in this Chapter:

   a. DSC All Ships Urgent or Safety Alerts shall be made on a VHF-FM base station or over MF/HF as dictated by the desired coverage area. All-Ship DSC Safety and Urgency calls are prohibited over MF/HF. The follow-on voice frequency/channel identification shall be included in the alert, and shall be the voice working frequency/channel corresponding to the selected DSC frequency.

   b. Once the DSC alert is sent, a transmitter shall be changed to the corresponding voice frequency and the follow-on voice announcement shall be made.

2. Weather Warnings. Weather warnings are transmitted upon receipt as a safety broadcast on MF, and from all VHF-FM sites identified in "National Weather Service Products Recommended for Broadcast" available from the link above.

   a. Changes to or reductions of this list, such as where CG VHF-FM R21 RFFs or other high level sites cover approximately the same geographic area as NWS VHF-FM sites, can be proposed by a representative to UNCLOG and will be decided by UNCLOG. Any proposed changes shall be submitted through district or area C4IT staff.

   b. The area commander may modify or suspend the broadcast schedule in an emergency or where operational responsibilities dictate provided UNCLOG is notified of the change. The CG does, however, retain the broadcast responsibility for weather and tsunami warnings as listed in the document.

3. Navigational Warnings. Navigational warnings are transmitted as safety broadcasts (see below) per broadcast instructions contained in the message.

Navigational warnings are intended to inform the mariner of important changes that affect the safety of navigation within a given AOR.

4. Urgent Messages. Urgent messages concern the safety of a ship, aircraft, other vehicle, or the safety of a person. The urgency signal should only be used to precede hurricanes, hurricane force winds, tsunami warnings, or other severe events as per World Meteorological Organization guidance.

5. Safety Messages. The safety signal shall precede a safety message broadcast. Safety messages contain important navigational or meteorological warnings, including space weather. Safety message broadcasts shall 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 message will normally consist of only one subject.

6. Scheduled Broadcasts. Scheduled MIBs may include search and rescue, navigational, hydrographic, and weather information. Safety and urgent messages that remain in effect at the next scheduled broadcast shall be repeated (see also section D regarding NAVTEX). Area and district commanders shall coordinate their broadcast times to minimize interference problems. HF, MF, and VHF-FM broadcasts shall be scheduled so that no interference will occur in overlapping coverage areas. Commandant (CG-652) shall be advised of any product or schedule changes that do not conform to the UNCLOG National Weather Service Products Recommended for Broadcast described in section A.1 of this Chapter. Area commanders shall publish scheduled MIB product content and broadcast times for each broadcast station in their Annex K to Area OPLAN. Any proposed changes shall be submitted through district or area C4IT staff.

7. Duration of Broadcasts. Textual length of messages for broadcast shall be kept to a minimum consistent with the need to pass important information. Urgent messages and other warnings may be broadcast on international distress and calling frequencies (MF 2182 kHz and VHF-FM Channel 16 (156.800 MHz)) provided the broadcast does not exceed one minute. An appropriate working frequency will be used to transmit messages requiring more time for transmission. Districts and units shall coordinate broadcasts with adjacent units to prevent interference with other broadcasts and operations.

8. Abbreviations. To reduce the broadcast time of MIBs, the originator shall use readily recognizable abbreviations as per Aids to Navigation Manual – Administration, COMDTINST M16500.7 (series).

   Note: If broadcasting NWS information, transmit the exact text received from the NWS.

9. Cancellations. It is the responsibility of the originator to cancel messages as soon as possible once action is no longer necessary. Furthermore, originators shall make every effort to provide a cancellation date on all issued MIBs where possible.

a. MIBs without a cancellation date always require a cancellation message. Originators shall issue weekly summaries of all active MIBs as per Aids to Navigation Manual – Administration, COMDTINST M16500.7 (series). These weekly summaries of active MIBs shall also serve to cancel all of the originators' MIBs not included in the summaries.

b. Originators of broadcasts shall review their active MIBs including broadcasts made by the NGA at CG request daily to avoid transmitting duplicate or outdated information.

10. Summary of Broadcast Requirements. Radiotelephone and NAVTEX broadcast scheduling guidance are provided in Exhibits 13-1, 13-2, and 13-3.

Exhibit 13-1
Atlantic Ocean, Gulf of Mexico, and Puerto Rico
NAVTEX Broadcast Schedules

Broadcast Station	Identifier	WX Broadcast Schedule (UTC)
Boston	F	0045, 0445, 0845*, 1245, 1645, 2045*
Portsmouth	N	0130, 0530, 0930*, 1330, 1730, 2130*
Charleston	E	0040, 0440, 0840*, 1240, 1640, 2040*
Miami	A	0000, 0400, 0800*, 1200, 1600, 2000*
San Juan	R	0200*, 0600, 1000, 1400*, 1800, 2200
New Orleans	G	0300*, 0700, 1100, 1500*, 1900, 2300
(*) Weather is normally broadcast four times per day. This symbol annotates the times when weather will not be broadcast.		

Exhibit 13-2
Pacific Ocean, Alaska, Hawaii, and Guam
NAVTEX Broadcast Schedules

Broadcast Station	Identifier	WX Broadcast Schedule (all times UTC)
Kodiak(#)	J X	0300, 0700, 1100*, 1500, 1900, 2300* 0340, 0740, 1140*, 1540, 1940, 2340*
Astoria	W	0130, 0530, 0930*, 1330, 1730, 2130*
San Francisco	C	0000, 0400*, 0800, 1200, 1600*, 2000
Cambria	Q	0045, 0445*, 0845, 1245, 1645*, 2045
Marianas	V	0100, 0500, 0900, 1300, 1700, 2100
Honolulu	O	0040, 0440*, 0840, 1240, 1640, 2040*
(#) Kodiak broadcasts weather forecasts during time slots formerly allocated to Adak. (*) Weather is normally broadcast four times per day. This symbol annotates the times when weather will not be broadcast.		

Exhibit 13-3
Radiotelephone/NAVTEX Broadcast Requirements

TYPE	Distress Voice 2182 kHz (MF) ---------- VHF-FM Channel 16 (156.800 MHz)	MF Voice Working 2670 kHz	VHF-FM Voice Working Channel 22/22A (157.1 MHz)	Distress NBDP NAVTEX 518 kHz
Scheduled Broadcasts	As scheduled	As Scheduled	As scheduled	As scheduled
Safety Broadcast	Preliminary Announcement (Note 2)	A C F	A C F	C E F IMPORTANT
Urgent Broadcast	Preliminary Announcement (Note 1,2)	A B D F	A B D F	E D F VITAL
Urgent Cancellation	Preliminary Announcement (Note 1)	A	A	E VITAL

A: Upon receipt,
B: Every 15 minutes for a 1 hour period.
C: Repeat next scheduled broadcast, unless canceled.
D: Repeat on scheduled broadcasts until canceled.
E: At first available period after receipt when frequency not in use.
F: Additional broadcasts as directed by originator.

CHAPTER 14 Note 1: Broadcast on 2182 kHz or VHF-FM Channel 16 (156.800 MHz) if less than one minute long. Otherwise broadcast on working frequency.

Note2: Preliminary announcement on Distress frequency - Continue on working frequency.

NAVTEX Subject Indicator Characters.

A Navigational warnings*
B Meteorological warnings*
C Ice reports
D Search and Rescue information*
E Meteorological forecasts
F Pilot service messages
G AIS
H LORAN messages
J SATNAV (e.g. GPS) messages
K Other radio-navigation service messages
L Navigational warnings - additional to letter A
V Special services – allocation by the IMO NAVTEX Panel
W Special services – allocation by the IMO NAVTEX Panel
X Special services – allocation by the IMO NAVTEX Panel
Y Special services – allocation by the IMO NAVTEX Panel
Z No messages on hand, or request for comments on broadcasts
(*) Cannot be rejected by receiver

B. Format of Marine Information Broadcast (MIB) and Messages.

1. Urgent Marine Information Broadcast (UMIB). Initial UMIB shall be preceded by a DSC call on the appropriate frequency/channel and shall include the frequency/channel of the follow-on voice broadcast. Subsequent broadcast(s) will be made on the appropriate frequency/channel. Operational commanders may direct that subsequent UMIBs be preceded by a DSC call if warranted.

   a. 2182 kHz and/or VHF-FM Channel 16 (156.800 MHz). PAN-PAN (3 times) (Pronounced "Pahn-Pahn") Name of called station or “ALL STATIONS” (3 times) THIS IS (voice call sign three times) and (MMSI once if initial announcement sent via DSC) (brief identifying data) LISTEN (2670 kHz or Channel 22A) OUT.

      (1) Urgent messages and other warnings may be broadcast on international distress and calling frequencies (2182 kHz and VHF-FM Channel 16 (156.800 MHz)) provided the entire broadcast does not exceed one minute (See section A.7 of this Chapter).

      (2) UMIBs normally broadcast on HF GMDSS frequencies must first be broadcast on the corresponding HF DSC frequency.

   b. 2670 kHz and/or VHF-FM Channel 22A (157.1 MHz). PAN-PAN (3 times) Name of called station or “ALL STATIONS” (3 times) THIS IS (voice call sign 3 times) and (MMSI once if initial announcement sent via DSC) BREAK (text) BREAK THIS IS (voice call sign once) OUT.

2. Cancellation Message. PAN-PAN (3 times) ALL STATIONS (3 times) THIS IS (voice call sign 3 times) and (MMSI once if initial announcement sent via DSC) BREAK PLEASE CANCEL URGENCY MESSAGE OF (date and time of message in UTC and brief identifying data on cancelled urgent traffic) BREAK THIS IS (voice call sign once) OUT.

3. Safety Marine Information Message Format.

   a. 2182 kHz and/or Channel 16. SECURITE (3 times) (Pronounced "SAY-CUR-I-TAY") Name of Called Station or “ALL STATIONS” (3 times) THIS IS (voice call sign 3 times) and (MMSI once if initial announcement sent via DSC) COAST GUARD MARINE INFORMATION BROADCAST (or) HURRICANE ADVISORY/STORM WARNING/THUNDERSTORM WARNING. LISTEN (2670 kHz or Channel 22A) OUT.

   b. 2670 kHz and/or VHF-FM Channel 22A (157.1 MHz).. SECURITE (3 times) Name of called station or “ALL STATIONS” (3 times) THIS IS (voice call sign 3 times) and (MMSI once if initial announcement sent via DSC) BREAK (text) BREAK THIS IS (voice call sign once) OUT.

4. Scheduled Broadcast Format.

   a. General.

      (1) HF automated broadcasts (Voice Broadcast Automation (VOBRA)), SITOR, radiofacsimile (radiofax) (see section E of this Chapter) require no preliminary announcement.

      (2) When no information is to be transmitted during a scheduled broadcast, the station shall make the following transmission after the call: "NO MARINE INFO BROADCAST THIS SCHEDULE. BREAK THIS IS (voice call sign once) OUT".

   b. 2182 kHz and/or VHF-FM Channel 16 (156.800 MHz). "ALL STATIONS" (3 times) THIS IS (voice call sign 3 times) COAST GUARD MARINE INFORMATION BROADCAST LISTEN (2670 kHz and or Channel 22A) OUT.

   c. 2670 kHz and/or VHF-FM Channel 22A (157.1 MHz). "ALL STATIONS" (3 times) THIS IS (voice call sign 3 times) BREAK (text) BREAK THIS IS (voice call sign once) OUT.

C. Other Broadcasting Procedures. To ensure proper transmission, the following precautionary measures and procedures shall be followed:

1. Units conducting broadcasts are cautioned on 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;

2. Radiotelephone broadcasts shall be made at a normal conversational speed but with the more important and more difficult portions (e.g., geographic coordinates of storms, forecast winds etc.) sent at reduced rate/speed to enable users to write down this information. Good diction is essential and the text shall be read in phrases rather than word by word;

3. Voice positions should be equipped with a system to mute the receiver when the microphone is keyed. Receivers not so equipped should be adjusted to minimize feedback;

4. Every effort shall be made to ensure scheduled broadcasts start on time and do not exceed authorized time periods; and

5. See section H of this Chapter for policy on broadcast monitoring.

D. Navigational Telex (NAVTEX).

1. Description. NAVTEX is a system for broadcasting NTMs, weather warnings and forecasts, ice warnings and other marine information on the internationally

designated frequency of 518 kHz, by automatic printout from a dedicated receiver. NAVTEX operational requirements are described in the NAVTEX Manual, International Maritime Organization MSC Circular 416. NAVTEX receivers are used on merchant and passenger vessels, offshore fishing vessels and pleasure vessels. Messages intended for broadcast over NAVTEX shall be formatted as per Chapter 12 of Aids to Navigation Manual – Administration, COMDTINST M16500.7 (series).

2. Administration. Area Commanders are the NAVTEX coordinators and shall ensure broadcasts are reliable, on schedule, within the prescribed duration, and to the extent practicable without interference. Commandant (CG-652) is the national NAVTEX coordinator.

3. Broadcast Schedule. CG broadcasts are conducted six times a day, with a normal duration of 20 minutes and a maximum duration of 40 minutes.

   a. The broadcast may exceed 40 minutes 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.

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

      (2) In cases where a broadcast is expected to exceed 40 minutes, all new messages must be transmitted during the first 40 minutes.

   b. All six scheduled broadcasts will have navigational warnings, if required. NTMs will be broadcasted for the period designated by the originator. Repeats of NTMs will be moved to the two daily broadcast slots where weather is not normally broadcast.

   c. Broadcast schedules for CAMSLANT and Sector San Juan should be coordinated since they overlap.

4. Priority Message Handling. Three message priorities are used to dictate the timing of the first broadcast of a new warning in the NAVTEX service. In descending order of urgency they are:

   a. 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 shall be stopped if possible to permit transmission of vital messages.

   b. 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.).

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

5. Information Control. Messages are sent in the order received and in order of priority, with all new messages going before old messages received but not previously broadcast. The last messages sent are those that were broadcast during the previous schedule. Messages being cancelled by a cancellation message shall be removed from the broadcast on which the cancellation message appears, and the cancellation message shall be removed from the broadcast queue after the broadcast.

   a. FEC idle signals shall be transmitted between each NAVTEX message to allow NAVTEX receivers to re-synchronize.

   b. Navigational warnings broadcast on NAVTEX normally include district NTMs and other information designated by the district. They normally do not include local warnings, detailed information on aspects that the oceangoing ship normally does not require, or NAVAREA, HYDROLANT, or HYDROPAC originated by the NGA.

   c. 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.

E. Other Automated Broadcast Systems. Certain HF Broadcast functions are automated through software application at the CAMS and COMMSTA Kodiak. These automated functions help assure broadcast schedules are met and that broadcasts are conducted consistently for high-seas mariners. Frequency assignment and broadcast schedule information is found in Annex K to Area OPLAN.

1. Voice Broadcast Automation (VOBRA). VOBRA provides computer-controlled, voice-synthesized broadcasts on HF at regularly scheduled times. VOBRA ensures all voice broadcasts are conducted at consistent speed and diction for maximum intelligibility for the high-seas maritime public.

2. Simplex Teletype Over Radio (SITOR). SITOR provides low-cost data transmission capability for high-seas mariners, and is used for broadcast of ice information, weather products, and hydrographic information in hard copy form. Currently only CAMSPAC (including Guam) and COMMSTA Boston provide this service to the public.

3. Radiofax. Radiofax is a service of the NWS, broadcast from CG CAMS and COMMSTA Kodiak. Radiofax automation is a function of NWS. Radiofax products are traditional weather charts for specific geographic areas.

4. Other Available Broadcasting Systems. Units that broadcast information via radio and data circuits other than those listed in this Manual are required to familiarize themselves with these systems and incorporate their use as necessary.

F. Marine Information Broadcast (MIB) and Service Changes/Casualties. It is essential that the CG notifies the maritime community of changes or outages in distress and safety related services. This notification shall include distress watch keeping and broadcasts of maritime safety information.

1. Changes, casualties, and casualty corrections concerning the following services shall be sent to the applicable CG broadcast station for broadcast as a NTM as per the Aids to Navigation Manual - Administration, COMDTINST M16500.7 (series):

   a. Sector 2182 kHz/ VHF-FM Channel 16 (156.800 MHz) watch-keeping.

   b. Safety broadcast on 2670 kHz/VHF-FM Channel 16 (156.800 MHz).

   c. District CC and SCC emergency telephone.

   d. MF/HF/VHF DSC capabilities

2. Changes, casualties, and casualty corrections concerning the following broadcast station services shall be sent to NGA NAVSAFETY WASHINGTON DC (primary) and NGA NAVSAFETY BETHESDA MD (secondary) for broadcast to NAVAREA IV (Atlantic), NAVAREA XII (Pacific), HYDROPAC (Guam), or HYDROLANT Navigation Warning:

   a. NAVTEX broadcasts;

   b. HF SITOR, HF voice, and HF Radiofax (Ice and Weather) broadcasts;

   c. SITOR on-call, HF Single sideband voice GMDSS guards; and

   d. Area CC emergency telephone and telex numbers.

3. In cases where district and area CCs are affected, notify:

   a. VIZADA via Telex
   Southbury Teleport – shift leader +1 203 262 5010
   Eik Teleport – eikvakt +1 47 51 40 80 00; and

   b. INMARSAT London UK via fax
   +44 0 20 7728 1142.

4. Changes or casualties to services or capabilities expected to last more than seven days shall be published via NTM.

G. Inmarsat All-Ships Search and Rescue Broadcasts. Shore-to-ship distress and search and rescue broadcasts may be made at no charge to all Inmarsat equipped ships in a

particular Inmarsat ocean region. Broadcasts shall be limited to those cases involving grave and imminent danger.

H. Broadcast Quality Control Monitoring Program.

1. Broadcast Quality Control Elements.

a. Transmission quality, particularly the communication procedures.

b. Product quality, formats, and content.

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

2. Program Description.

a. Area commanders shall establish a monitoring and customer feedback program for all MIBs (e.g., 1 800 numbers and internet Web pages) with the goal of improving MIB communication procedures.

b. Area commanders shall engage the CG AUX where appropriate to assist in these efforts. Such engagement shall be initiated and managed through the Auxiliary Department of Operations Telecommunications Division at the national level (AUX-DVC-OT) who will designate an Aux Command POC for the appropriate CAMS.

c. All communication facilities making MIBs shall 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" shall be the guiding principle in this review. Suggestions for improvements in content or format shall be submitted to the originating agency. Suggestions for changes in broadcast time, frequencies, or for equipment shall be submitted to UNCLOG via the chain-of-command.

d. NAVTEX, HF SITOR, HF Radiofax, Inmarsat SafetyNET, and HF/MF voice broadcasts shall be monitored continuously for quality by each CAMS and COMMSTA Kodiak.

e. All sectors shall monitor their broadcasts for quality on a random basis at least weekly.

f. In addition, commanding officers of units that broadcast maritime safety information shall measure transmitter performance at least weekly. Such measurements shall include, and as allowable with currently installed equipment, measurement and verification of transmitted power, voltage standing-wave ratio (VSWR), carrier frequency, and where applicable mark/space tone placement, frequencies, and tolerances.

APPENDIX A ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS)

A. Roles and Responsibilities. CG personnel installing, operating, and/or maintaining communication systems and cryptographic systems, shall comply with current COMSEC or NIST publications and directives as applicable. The primary source and reference of EKMS policy and procedures is EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3. CG specific EKMS policy and procedures are promulgated by numbered USCG COMSEC Advisory messages and are effective until incorporated into this Manual and EKMS-1. CG personnel performing COMSEC related duties shall be thoroughly familiar with and have access to EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3. CG personnel are responsible for immediately reporting any irregularities that may affect COMSEC materials as per EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3. Roles and responsibilities, selection and designation criteria, and training requirements are contained in EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3, Chapter 4.

1. Command, Control, Communications, Computers and Information Technology Service Center (C4ITSC) (BOD-IAB). The C4ITSC (BOD-IAB) promulgates detailed CG COMSEC/EKMS policy and exercises service-wide management and oversight of CG EKMS accounts. The C4ITSC (BOD-IAB) works in close cooperation with the NSA, CNO, Naval Communications Security Material System (NCMS), and the EKMS Tier 1 entities to ensure that all CG EKMS accounts have the necessary COMSEC resources to operate effectively. Additionally, the C4ITSC (BOD-IAB) coordinates internationally with coalition partners through 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.

    a. The C4ITSC (BOD-IAB) shall be responsible for updating and issuing, in coordination with Commandant (CG-65), EKMS policy requirements throughout the CG.

    b. The C4ITSC (BOD-IAB) serves as the COMSEC ISIC and service authority for all CG COMSEC (EKMS) accounts. However, account managers shall first contact their area or district ISIC on COMSEC matters. The C4ITSC (BOD-IAB) is also responsible for the CG EKMS Inspection Program.

    c. The C4ITSC (BOD-IAB) also functions as the CG command authority for modern key under the EKMS Central Facility and the controlling authority for all CG controlled keys, including those comprising the national level JIACC KEYMAT Package.

2. Area Commanders. Area commanders shall assist in the management of the CG EKMS Program as follows:

a. Designate in writing an EKMS ISIC to serve as an EKMS inspector and assist CG commands in managing their EKMS Accounts. EKMS ISIC responsibilities are outlined in Chapter 4 of EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3. Area commanders shall coordinate Navy/CG EKMS support requirements with the appropriate USN fleet commander and promulgate area specific COMSEC instructions, requirements and procedures.

b. Initiate corrective actions as appropriate in response to COMSEC incidents.

c. Ensure compliance with the Continuous Evaluation Program (CEP) as described in Personnel Security and Suitability Program, M5520.12 (series).

3. District Commanders. District commanders shall direct their units as per area COMSEC instructions, and address their COMSEC needs to the cognizant area commander.

a. District commanders may designate district EKMS ISICs to assist area EKMS ISICs as inspectors and to assist CG accounts within their AOR in managing their EKMS accounts as needed.

b. Initiate corrective actions as appropriate in response to COMSEC incidents.

c. Ensure compliance with the Continuous Evaluation Program (CEP) as described in Personnel Security and Suitability Program, M5520.12 (series).

4. Commanding Officers. Commanding officers are responsible for maintaining a comprehensive COMSEC program at their commands. Unit commanding officers are responsible for the manner in which their personnel perform EKMS/COMSEC duties, at a minimum, commanding officers shall:

a. Be thoroughly familiar and comply with the specific responsibilities and duties and required inspections as outlined in Chapter 4, article 450 of EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3;

b. 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

c. Ensure compliance with the CEP as described in Personnel Security and Suitability Program, M5520.12 (series).

5. EKMS Account Manager/Alternate Account Managers. EKMS account managers/alternates are equally responsible for all actions associated with the receipt, handling, issue, safeguarding, accounting, disposition and management of COMSEC material assigned to an EKMS account and also serves as the commanding officer's primary advisor on EKMS account management matters.

Specific responsibilities and duties are detailed in Chapter 4, Article 455 of EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3.

6. Local Element Personnel. Local element personnel are responsible to their commanding officer for the proper management and security of all COMSEC material assigned to them. Specific duties are outlined in EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3, Chapter 4, Article 465.

B. Electronic Key Management System (EKMS) Inspections. EKMS inspections are the responsibility of the respective area/district ISIC. More detailed inspection guidelines are listed in the Electronic Key Management System Inspection Manual, EKMS 3(series).

C. Communication Security (COMSEC) Material Control System (CMCS). The CMCS is the overall national system for the distribution, use and control of COMSEC equipment, KEYMAT and aids used to protect official government classified and SBU information. The CMCS provides for the physical security of COMSEC material. The CMCS has two major components; the EKMS and the Vaults, Depot and Logistics System (VDLS).

1. Electronic Key Management System (EKMS). The EKMS is used for the accounting and management of cryptographic equipment and physical KEYMAT, and the production, accounting, management and distribution of electronic KEYMAT. Major components of the EKMS are the Local COMSEC Management System (LCMS), a software application, and the local management device (LMD), the hardware platform, and key processor (KP), the cryptographic device. LCMS provides the capability for automated generation, accounting, distribution, destruction, and management of electronic key, as well as management of physical key and non-key COMSEC related items. DON provides the vast majority of CG COMSEC equipment and acts as the Central Office of Record.

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.

D. Key Management Infrastructure (KMI). All parts – computer hardware, firmware, software, and other equipment and its documentation; facilities that house the equipment and related functions; and companion standards, policies, procedures, and doctrine that form the system that manages and supports the ordering and delivery of cryptographic material and related information products and services to users. The KMI is intended to eventually replace the EKMS.

E. Inspections. Area and district EKMS ISICs shall perform inspections of EKMS accounts under their cognizance as per EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3 and the EKMS Inspection Manual, EKMS 3 (series). The C4ITSC (BOD-IAB) will conduct inspections of EKMS accounts held by headquarters units. EKMS accounts shall be inspected at least every 24 months. Accounts may prepare for inspections by referring to the EKMS account self assessment included in EKMS Inspection Manual, EKMS 3 (series).

F. Electronic Key Management System (EKMS) Training Visits. All EKMS accounts are required to receive a periodic NCMS Advice and Assist (AA) Training Visit no later than 90 days prior to the next scheduled formal inspection. The date of the latest training visit should be located in the account correspondence and message file. EKMS Managers are encouraged to take advantage of additional NCMS AA training team services as promulgated by the regional AA team monthly message.

G. Maintenance of Cryptographic Equipment. Commands are responsible for ensuring proper cryptographic maintenance and repair. Repair of USN owned cryptographic equipment shall be accomplished as per the EKMS-5 (series) Cryptographic Equipment Information/Guidance Manual. Inoperative equipment shall be repaired or replaced by the servicing crypto repair facility (CRF) or other repair/maintenance facility. EKMS Managers should review EKMS-1 (series) EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3 for specific procedures. Repair and replacement of all cryptographic equipment shall be coordinated through the C4ITSC (BOD-IAB).

APPENDIX B COAST GUARD RECORD MESSAGING SYSTEM (CGRMS)

A. General. This Appendix applies to operational use of the CGRMS.

B. Coast Guard Record Message System (CGRMS). CGRMS is comprised of several subsystems for processing both classified and unclassified record message traffic. CGRMS provides routing to various CG and non-CG commands, units and agencies throughout the CG. Classified CG Message System (C-CGMS) is available via the SIPRNET system for processing classified record messages. Extensive information and resources on CGRMS are available on the CG Portal.

1. Department of Defense (DOD) Networks.

   a. Defense Message System (DMS) and Automated Message Handling System (AMHS). DMS is an organizational messaging system developed by the DOD based on commercially available software.

   b. Message Distribution Terminal (MDT). The MDT is the sole remaining component of the legacy Automatic Digital Network (AUTODIN) still in use by the CG. AUTODIN remains in use by DOD and other federal agencies, and provides for the transmission of narrative and data pattern traffic on a store-and-forward basis.

   c. Fleet Secure Internet Protocol Router Network (SIPRNET) Record Messaging.

      (a) Fleet SIPRNET messaging (FSM) a system located at each NCTAMS that allows afloat units to receive record messages over SIPRNET. The receive function of FSM allows Naval Modular Automated Communications System (NAVMACS II) equipped cutters to receive record message traffic from their servicing NCTAMS via SIPRNET. These record messages are received via NAVMACS and profiled to a public folder on SIPRNET for viewing.

      (b) The transmit function of FSM allows NAVMACS equipped cutters to transmit record message traffic to their servicing NCTAMS via SIPRNET. Record messages are drafted using SIPRNET CGMS, digitally signed public key infrastructure (PKI) and e-mailed to the servicing NCTAMS. The software PKI certificate is assigned to each authorized releaser via the cutter's trusted agent. The record message must be correctly formatted for the servicing NCTAMS to process the record message.

      (c) Two-way FSM involves an Inmarsat path for record message delivery rather than legacy MILSATCOM circuits such as CUDIXS and Fleet Satellite Broadcast (FSB).

2. Record Message Preparation. Record messages may be prepared as per the format contained in Communications Instructions-Teletypewriter (Teleprinter)

Procedures, ACP 126 (series). Alternately, GENADMIN formatting may be used. GENADMIN formatting instructions and record message map are found in Telecommunications Users Manual, NTP 3 (series) Appendix A.

a. If GENADMIN formatting is used, avoid combining with modified ACP 126 (series) formatting.

b. CGMS is used to prepare GENADMIN-formatted record messages.

c. Certain record messages under United States Message Text Format (USMTF) are required of CG units, e.g., CASREP, MOVREP, SORTS, and certain others as directed by operational commanders. In most cases, refer to Operational Reports, NWP 1-03.1 (series) for formatting and content requirements. Otherwise, refer to the publications directed by the operational commander.

3. Heading. The record message heading provides precedence, unique identity, and delivery information (addressees) for the record message.

a. Precedence. The precedence enables record message drafters to indicate the relative order of processing and delivery, affected by automated record message processing systems in the same manner as formerly performed manually by telecommunication personnel. The precedence of an incoming record message has no direct effect on the time in which a reply must be sent or on the precedence assigned to that reply. There are five precedence categories: routine, priority, immediate, flash and emergency override (reserved for flag level/Joint Chiefs use only). The assignment of precedence is the drafter's responsibility, although the releaser may either confirm or change the assignment. Do not assign a higher precedence than is necessary.

(1) Single Precedence. In a record message containing only one precedence, the precedence applies equally to all addressees, whether or not information addressees are included in the message heading.

(2) Dual Precedence.

(a) In the case of a record message containing action and information addressees, if possible use dual precedence to indicate a lower precedence for information addressees than for action addressees to ease the burden on record message processing systems with respect to higher precedence record messages in the system.

(b) Dual precedence applies to record messages with the primary precedence of priority or above. In all cases of dual precedence assignment, the secondary precedence must have less of a criteria category assigned than the primary precedence assigned.

(c) Do not use dual precedence in record messages containing no Information addressees.

(3) System Processing. A record message processing system handles outgoing record messages in order of precedence and entry into the message queue. For example, a queue with ten priority record messages pending which receives an immediate for transmission will handle the immediate before the next priority in the queue.

(4) Criteria for Assignment of Precedence. Exhibits B-2 through B-5 lists precedence categories and their criteria, with examples of each.

Exhibit B-2
Flash Precedence Assignment Criteria

Designation	Prosign	Definitions and Examples
Flash	Z	Flash precedence is reserved for initial enemy contact messages or operational combat messages of extreme urgency. Authority to release flash record messages is restricted to flag and general officers, civilian equivalents, or commanders or their representatives specifically authorized in writing. Brevity is mandatory. Examples include: (1) Initial enemy contact reports; (2) Messages recalling or diverting friendly aircraft about to bomb targets unexpectedly occupied by friendly forces; or messages taking emergency action to prevent conflict between friendly forces; (3) Warning of imminent large scale attacks; (4) Extremely urgent intelligence messages; (5) Messages containing major strategic decisions of great urgency; and (6) Tropical storms, typhoons, or hurricanes believed to be previously undetected. Commanders may use flash precedence for reporting, provided there are no extenuating circumstances that would jeopardize the tactical situation.

Exhibit B-3
Immediate Precedence Assignment Criteria

Immediate	O	Immediate is the precedence reserved for very urgent record messages relating to situations which gravely affect the security of national/allied forces or populace. Examples include: (1) Amplifying reports of initial enemy contact; (2) Reports of unusual major movements of military forces of foreign powers in times of peace or strained relations; (3) Messages which report enemy counterattack which request or cancel additional support; (4) Attack orders to commit a force in reserve without delay; (5) Messages concerning logistical support of special weapons when essential to sustain operations; (6) Reports of widespread civil disturbance; (7) Reports of warning of grave natural disaster (e.g., earthquake, flood storm); (8) Request for, or directions concerning, distress assistance; (9) Urgent intelligence messages; (10) Aircraft movement reports (e.g., messages relating to requests for news of aircraft in flight, flight plans, cancellation messages to prevent unnecessary search/rescue actions); and (11) Weather observations with wind speed of 34 knots or greater.

Exhibit B-4
Priority Precedence Assignment Criteria

Priority	P	Priority is the precedence reserved for record messages concerning the conduct of operations in progress and for other important and urgent matters when routine precedence will not suffice. Examples include: (1) Situation reports on position of front where attack is impending or where fire or air support will soon be placed; (2) Orders to aircraft formations or units to coincide with ground or naval operations; (3) Administrative, logistical, and personnel matters of an urgent and time sensitive nature. No higher than priority precedence will be assigned to administrative messages except those reporting death, serious illness, or serious injury, which will be assigned immediate precedence; (4) Weather observations with surface wind speed 33 knots or less, and all oceanographic observations; and (5) Messages concerning movement of naval, air, and ground forces.

Exhibit B-5
Routine Precedence Assignment Criteria

Routine	R	Routine is the precedence to be used for all types of record messages which justify transmission by rapid means but are not of sufficient urgency and importance to require a higher precedence. Examples include: (1) Messages concerning normal peace time military operations, programs, and projects; (2) Messages concerning stabilized tactical operations; (3) Operational plans concerning projected operations; (4) Periodic or consolidated intelligence reports; (5) Troop movement messages, except when time factors dictate use of a higher precedence; (6) Supply and equipment requisition and movement messages, except when time factors dictate use of a higher precedence; and (7) Administrative, logistics, and personnel matters.

(5) Speed of Service Objective (SOSO). Exhibit B-6 displays the "writer-to-reader" record message precedence timeframes applicable for legacy systems.

Exhibit B-6
Speed of Service Objectives (SOSO) for Legacy Systems

Precedence	Prosign	SOSO
Flash	Z	As fast as possible with a goal of less than 10 minutes.
Immediate	O	30 Minutes.
Priority	P	3 Hours
Routine	R	6 Hours or start of next business day.

b. Date Time Group (DTG). The DTG, in conjunction with the originator uniquely identifies the record message. For this reason, it is important not to

duplicate the DTG within the same command. The DTG immediately follows the precedence, separated by a single space. The DTG is composed of the calendar date in two digits, the time in UTC (indicated by Z), the month in three letter abbreviations, and the year in two digits.

c. Originator. The originator of a record message is the command by whose authority a message is sent. The originator in the heading of a record message is represented by a PLA, and appears at the 'from' line (FM). The PLA must be correct for proper record message handling. The Diversified PLA Verification System (DPVS) is embedded in CGMS, and can be used to ensure the correct PLA is entered in the FM line.

d. Action Addressee. Action addressees are those addressees from which a reply or specific action in response is expected, or which have primary interest in the content of the message. The action addressee is represented by a PLA, and this line is designated by the prosign TO. Additional action addressees appear below the first action addressee.

(1) PLAs must be correct for delivery to intended recipients.

(2) Collective addresses (i.e., AIG, CAD, TASKs) may appear as action addressees only.

(a) Staff symbols are used to aid in correct routing of messages to appropriate folders. They serve an administrative function that reduces the amount of irrelevant traffic being viewed by particular divisions or personnel.

(b) Staff symbols are listed in enclosure 2 of the Standard Distribution List, COMDTNOTE 5605.

(c) For CG messages sent to USN PLAs, use //JJJ// if the office code is not known.

e. Information Addressee. Information addressees are those addressees from which no reply or specific action in response is expected, but at least have a secondary interest in the content of the record message. The information addressee is represented by a PLA, and this line is designated by the prosign INFO. Additional information addressees appear below the first information addressee.

(1) PLAs must be correct for delivery to intended recipients.

(2) Collective Addresses may not appear as information addressees.

f. Exempt Addressee. Exempt Addressees are used when addressing a record message to a collective addressee (AIG, CAD, or TASK), but delivery of the record message to certain members of that AIG, CAD, or TASK is not

desired. The PLAs for those members are entered in the record message heading as exempt, identified by the prosign XMT.

(1) PLAs entered under XMT must be correct to prevent delivery of a record message addressed to an AIG, CAD, or TASK to the addressees the PLAs represent.

(2) Exempt addressees are never used in messages which do not contain an AIG, CAD, or TASK in the heading.

g. Accounting Symbol. The accounting symbol is no longer used in the drafting of messages.

4. Separation. The first separation serves to separate the heading from the text of a record message, and is identified by the prosign BT.

5. Text. The text of the record message contains the substance of the information being conveyed by the record message.

a. Classification. The first line of the text is always the record message classification.

(1) The classification shall appear as follows:

(a) UNCLAS;

(b) C O N F I D E N T IA L;

(c) S E C R E T; or

(d) T O P S E C R E T.

(2) When using unclassified CGMS, only 'UNCLAS' is available for the classification line (with or without the FOUO caveat). Encrypted for Transmission Only (EFTO) is no longer authorized for use. When using classified CGMS, users can select from all four classification levels.

b. Standard Subject Indicator Code (SSIC). Standard Subject Identification Codes (SSIC) Manual, COMDTINST M5210.5 (series) contains a complete list of SSICs in use in the CG.

c. Subject Line. All CG originated narrative record messages, with the exception of Service record messages, shall contain a subject line, indicated by the characters "SUBJ:" followed by the subject of the record message. The subject will be a brief description of the general topic of the record message.

d. Reference Line. Identify previous record messages, Instructions, Manuals, or other forms of official correspondence, including memoranda, E-mail, phone conversations, and conferences, in the reference line. In the case of record message references, if not all addressees are addressed in the referenced

record message, append the reference with "NOTAL", defined as "not to all addressees."

(1) Identify references sequentially beginning with 'A.'

(2) Record message references shall include the referenced message originator's complete and correct PLA (exceptions appear below) followed by the DTG, month, and year. Precedence and office codes are not included in references.

(3) In the case of a record message containing only one action addressee which includes a referenced message originated by that addressee, the word 'YOUR' may be substituted for the PLA in that reference.

(4) Record messages containing references originated by any Information addressee, or by any non-addressed PLAs, must in all cases include the referenced record message originator's PLA in the reference.

(5) Record message originators referencing their own record messages may substitute the word 'MY' for the PLA in the reference.

(6) Sample references appear in Exhibit B-7.

Exhibit B-7
Sample References

Reference Type	Sample Reference Format
Record Message: Reference appearing in message containing single Action addressee, from which reference originated.	YOUR 011500Z JAN 12
Record Message: Reference appearing in message containing two or more Action addressees, or reference originated by any Information addressee or by any unit not addressed in referencing message.	COMDT COGARD WASHINGTON DC 011500Z JAN 12
Record Message: Reference originated by same unit as message in which reference appears.	MY 011500Z JAN 12
Directive	TELECOMMUNICATION MANUAL, COMDTINST M2000.3E, CH. 1, PAR. 3B
Memorandum	COMDT (CG-65) MEMO 2000 OF 15 MAY 011
E-Mail	E-MAIL FROM CAPT A.B. SEA, COMDT (CG-65) DATED 1 JAN 12
Phone Conversation	PHONCON CAPT A.B. SEA, COMDT (CG-65) AND CAPT R.U. SHORE, LANTAREA (LANT-6) OF 15 JAN 12
Conference	WATERSIDE CONFERENCE, NCTAMS LANT NORFOLK VA, 1 JAN 12

(7) The record message text is the responsibility of the drafter. To keep consistency in CG correspondence, the text format of record messages shall be in as per The Coast Guard Correspondence Manual,

COMDTINST M5216.4 (series), for format. Chapter 10 of this Manual may also be used for record message text preparation. Lines of text are limited to sixty-nine characters from left margin, including spaces. CGMS handles this automatically; no returns are required while entering text within a paragraph or sub-paragraph. Sub paragraphs should be indented at least two spaces.

6. Separation. The second separation serves to separate the record message text from the end-of-message functions, and is identified by the prosign BT.

7. Attachments. CGMS allows the use of attachments strictly within the CGMS network. Record messages addressed to PLAs outside of the CGMS network (e.g., cutters with their record message guards with USN units, or any non-CG PLAs), will have all attachments stripped from those record messages.

APPENDIX C RESCUE 21 SYSTEM CONFIGURATIONS

A. Rescue 21 (R21) System Configuration. R21is a GMDSS compliant command, control, and communication (C3) system operating within sea area A1 as defined in Chapter 12 of this Manual. Standard and consistent system configuration is essential. Each sector commander shall designate a minimum of two personnel as local R21 system supervisors. The systems supervisors are responsible for R21 configuration management including maintenance of locally established optional setups within R21 for the sector and its stations. R21 configuration shall not be adjusted by individual watchstanders except as authorized by the sector commander or his/her designated appointee.

B. Permission Levels. Within R21, users are granted various permission levels. System supervisors will have full accessibility to assign these functions. The sector commander must ensure a system supervisor is available at all times to export data from the system. The SCC may designate additional personnel to have the system supervisor permission level. This permission level should be limited to fully qualified R21 watchstanders.

C. Rescue 21(R21) Initial Log-in Screen Set-up. Upon login to the system, the following screens, at a minimum, must be opened and accessible at all times, either minimized or displayed.

1. Geo Display;
2. Audio Manager;
3. System Manager; and
4. DSC Manager.

D. Rescue 21 (R21) Log-off Policy. During watch relief at those units with distress frequency guard requirements, at least one computer shall be operational so that the system, i.e. radio, can be constantly monitored. At a minimum, the following columns on the DSC Panel shall be active:

1. Call time;
2. Station (RFF on which the call was received);
3. Received quality indication (RQI)—strength of the received signal);
4. Format (individual, multi, all ships);
5. Category (e.g., urgency, routine,);
6. TeleCmd1 – Right click on the column and select position (position shall be checked at all times);
7. From (MMSI number);

8. Nature (nature of distress);

9. Position;

10. Receiving frequency; and

11. Transmitting frequency.

E. Rescue 21 (R21) Remote Fixed Facility (RFF) Determination. Default RFF determination for DSC alert acknowledgement is based on RQI and received signal strength indication (RSSI).

F. Rescue 21 (R21) Geo Display. The Geo Display visually displays the SCC's AOR. Displayed on this screen are lines of bearing (LOB), fixes, SCCs, RFFs, stations, etc. The LOBs are displayed when the selected channel(s) for DF are keyed by a VHF-FM radio. The LOB decay time shall be determined in the SCC SOPs. At a minimum, upon start-up of the Geo Display, the following layers must be checked (if available):

1. R21;

2. CG AOR; and

3. Latitude/longitude grid (5x5).

G. Rescue 21 (R21) Radio Logs. Do not use the R21 incorporate log or R21's Incident Manager Function.

H. Rescue 21 (R21) Radio/Channel Configuration. Each RFF site has six radios, each of which contain sixteen available "slots" or positions in which to program "code plugs," which are the channel/frequency information programmed into the radio. Not all positions are used. Radio configuration is as follows:

1. Radio 1. VHF-FM Channel 16 (156.800 MHz) guard only, transmit/receive;

2. Radio 2. VHF (1), transmit/receive. All 16 positions are available for use, channel/frequency plans are the responsibility of the respective area;

3. Radio 3. VHF (2), transmit/receive. All 16 positions are available for use, channel/frequency plans are the responsibility of the respective area;

4. Radio 4. UHF, transmit/receive. All 16 positions are available for use, channel/frequency plans are the responsibility of the respective area;

5. Radio 5. VHF-FM Channel 70 (156.525 MHz), DSC only; and

6. Radio 6. Asset tracking (not yet used).

I. Rescue 21 (R21) Archive Tapes. Personnel access to the playback archives shall be determined by the system supervisor.

1. The weekly on-site and off-site tapes should be rotated every seven days. The on-site tapes should be stored within the SCC. The off-site tapes should be stored in a secure space outside the SCC building. The locations chose to store the on and off-site tapes should be included in the SCC SOP.

2. All recorded data on the tapes shall be retained for at least 30 days.

3. If a tape contains transmissions of a significant case, mark the tape with the case name, dates, and times the communication took place and set aside pending the completion of review, litigation, investigation etc. Retain as per Chapter 6.

4. Tapes shall be stored as per the following requirements:

   a. Keep tapes in their plastic containers when not in the tape drive.

   b. Keep the tapes in a humidity- and temperature-controlled environment. If the archive environment is substantially different than the tape drive, allow a reasonable acclimation period before loading.

   c. Tape quality must be checked before reusing. Assure that the tape is not damaged, i.e., wrinkled, burnt, stretched, etc.

J. Rescue 21 (R21) System Alerts. System alerts notify the General Dynamics Customer Care Center (CCC) that there is a problem with the R21 equipment.

1. The CCC will manage system problems, notify the region/sector affected, and provide the affected SCC an estimated time of repair.

2. If the CCC notifies the SCC that an RFF has been identified with a communication problem then the operations/communication unit watchstander shall notify the district, and other commands of the RFF malfunction per the SCC SOP.

3. Operators can view system status by reviewing the system manager panel, which displays the current status of SCCs', RFFs', and stations' equipment and communication capabilities.

4. At a minimum, the following system alerts shall be active in the 'system alerts' panel (additional guidance may be provided in Annex K to Area OPLAN, district supplement, or sector SOP):

   a. Asset tracking failure (when available);

   b. Asset failed to report (when available);

   c. RFF status update;

   d. Station status update;

   e. SCC status update; and

f. RFF intrusion.

K. Rescue 21 (R21) System Failures. In the event an R21 equipment failure occurs but the CCC does not acknowledge the alert, the operations or communication unit watchstander shall call the CCC (877-449-0600). The CCC will then call the General Dynamics field service technician (FST) to respond, troubleshoot, and identify failed equipment, and to pick up, deliver, and install the replacement equipment.

1. Once the SCC operations unit watchstander has notified the CCC, the watchstander shall continue with the notifications procedures to ensure all necessary parties in the chain-of-command are made aware of the situation as outlined in current policy, including CASREPs, etc.

2. Station operators shall notify the SCC, who will notify the CCC, of any hardware equipment casualty and shall continue with the notifications procedures outlined in current policy, i.e., CASREPs.

3. Casualty reports are required if an outage cannot be repaired within 12 hours and the casualty diminishes the ability to adequately cover the entire AOR.

L. Rescue 21 (R21) Automated Broadcasting. Broadcast formats and contents remain the same. It is only how the broadcast is sent that will change.

1. The communication unit watchstander has three options of sending out a broadcast:

   a. Select a channel & RFF and transmit (live voice broadcast);

   b. Record a voice broadcast (for later broadcast); or

   c. Type a broadcast for the voice synthesizer.

2. The communications unit watchstander shall replay all recorded or synthesized broadcasts prior to the first transmission to ensure that the record message is clear and that all the words are pronounced correctly and clearly.

3. All broadcasts shall be logged.

4. R21 policy requires certain types of information be broadcast simultaneously on all RFFs to ensure the entire AOR is covered. However, this broadcast method may produce varying levels of echoing and distortion, thought to be minimal. Report service degradation issues caused by the simultaneous broadcast method via the chain-of-command to Commandant (CG-65).

5. All UMIB's shall be sent per Chapter 13 of this Manual upon receipt. Automated broadcasts will only be used for subsequent transmissions of a UMIB.

6. Certain types of broadcast information require simultaneous broadcasting on all RFFs to ensure the entire AOR is covered. This policy remains in effect under the new R21 system. However, using this broadcast method with new R21

technology and capability may produce varying levels of echoing and signal distortion. It is expected that the levels of echoing and signal distortion will be minimal. If units experience a significant degradation of service to the maritime public as a result of using the simultaneous method of broadcasting, the specific incidents should be documented and a report sent via chain-of-command to Commandant (CG-65).

M. Direction Finding (DF) Channels. DF is permanently assigned to Channel 16 (156.800 MHz). One other channel can be selected for DF capability, i.e., the CG working channel an asset is using.

1. Secondary R21 DF receivers shall remain tuned to Channel 70 DSC (156.525 MHz) unless temporarily tuned to 121.5 MHz or to a different VHF working channel to meet other operational needs.

2. The secondary DF can locate transmissions on 121.5 MHz, 243 MHz, and Channel 70 DSC (156.525 MHz) provided it is within the line of sight. No audio will be received; the DF function provides LOB only.

   Note: Some RFF's are outfitted with filtering systems that may limit the ability to receive these signals.

N. Direction Finding (DF) Functionality Testing. Units shall conduct functionality testing every 12 hours with an adjacent RFF(s). If there is no adjacent RFF within range then a DF accuracy test shall be conducted with a CG asset that provides DGPS coordinates once per day when possible.

O. Recording and Immediate Playback. All communication within the R21 system is recorded and available for immediate playback.

1. If a received transmission is garbled or inaudible then the operations/ communication unit watchstander should use the R21 band pass filter to omit some of the white noise heard in a transmission and/or manipulate the speed of the transmission to further clarify the call. The original, unchanged file must also be saved for case documentation prior to saving with the alterations. The file name must not be changed to avoid possible corruption of the .wav file.

2. If the transmission is still unreadable then the operations unit watchstander shall extract the .wav files onto a CG approved device (i.e. portable encrypted hard drive) and input the transmission into the Goldwave system for additional clarity.

P. Predetermined Maximum Theoretical Range. Each RFF shall be maintained in the local SOP and submitted to the district and area CCs for addition to area and district SAR plans.

1. The maximum theoretical range will be based on the RFF receive antenna heights and use the following computation for radio line of sight communications: $\sqrt{}$antenna height x 1.23 = max theoretical range.

2. A second maximum theoretical range will be contained in each publication that includes the max theoretical range of an unknown vessel calling with a 30' antenna using the following computation: RFF max theoretical range + √30' antenna x 1.23 = combined max theoretical range of distance with unknown vessel.

APPENDIX D GLOSSARY OF ACRONYMS AND TERMS

--- (A) ---

AA	Advice and Assist
ACCB	Aviation Configuration Control Board
ACP	Allied Communications Publication
ACKNLDG	Acknowledge, Record Message Prosign
AES	Advanced Encryption System
AIG	Address Indicating Group
AIM	Aeronautical Information Manual
AIRSTA	Air Station
AIS	Automatic Identification System
AIS-SART	Automatic Identification System-Search and Rescue Transmitter
ALC	Aviation Logistics Center
ALCGCIV	All Coast Guard Civilian, General Record Message title
ALCGENL	All Coast Guard Enlisted, General Record Message title
ALCGFINANCE	All Coast Guard Finance, General Record Message title
ALCGOFF	All Coast Guard Officer, General Record Message title
ALCGPSC	All Coast Guard Personnel Service Center, General Record Message title
ALCGRECRUITING	All Coast Guard Recruiting, General Record Message title
ALCGRSV	All Coast Guard Reserve, General Record Message title
ALCOAST	All Coast Guard, General Record Message title
ALCOM	All Commands, General Record Message title
ALE	Automatic Link Establishment
ALPACFLT	All Pacific Fleet, General Record Message title
ALTERS	Allied Telecommunications Record System
AMHS	Automated Message Handling System
AMVER	Automated Mutual-Assistance Vessel Rescue
AOR	Area of Responsibility
ATC	Air Traffic Control
ATP	Allied Tactical Publication
ARQ	Automatic Repeat Request
AUTODIN	Automatic Digital Network
AUX	Auxiliary
AWC	Area-Wide Communication Center

--- (B) ---

BNM	Broadcast Notice to Mariners
BSU	Base Support Unit
BT	Break, Record Message Prosign

--- (C) ---

C3	Command, Control and Communications
C3CEN	Command, Control and Communications Engineering Center, Portsmouth VA
C4I	Command, Control, Communication, Computer, and Intelligence
C4ISM	Command, Control, Communication, Computer, Intelligence, Sensor Analysis and Data Mining
C4ISR	Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance
C4IT	Command, Control, Communication, Computers and Information Technology
C4&IT	Command, Control, Communication, Computers and Information Technology
C4ITSC	Command, Control, Communication, Computers and Information Technology Service Center
CAD	Collective Address Designator
CAMS	Communication Area Master Station
CAMSLANT	Communication Area Master Station Atlantic
CAMSPAC	Communication Area Master Station Pacific
CART	Command Assessment of Readiness and Training
CASREP	Casualty Report
CAT	Communications Assist Team
CBP	Customs and Border Protection
CBUC	CAMS Back-Up CAMS
C&CC	Command and Control Center
CC	Command Center
CCC	Customer Care Center
C-CGMS	Classified Coast Guard Message System
CCI	Cryptographically Controlled Item
CCMG	Continuity Communications Managers Group
CEP	Continuous Evaluation Program
C.F.R	Code of Federal Regulations
CG	Coast Guard
CGCIRT	Coast Guard Computer Incident Response Team
CGCYBERCOM	Coast Guard Cyber Command
CGFSM	Coast Guard Fleet SIPRNET Messaging
CGMS	Coast Guard Message System
CGOne	Coast Guard One Network
CGRMS	Coast Guard Record Messaging System
CGSW	Coast Guard Standard Workstation
CGTS	Coast Guard Telecommunication System
CIA	Communication Information Advisory
CIB	Communication Information Bulletin
CIC	Combat Information Center
CIL	Critical Information List

CIRM	International Radio Medical Center
CIRM ROMA	International Radio Medical Center, Roma, Spain
CJCS	Chairman, Joint Chiefs of Staff
CMCS	COMSEC Material Control System
CMS	COMSEC Material System
CND	Computer Network Defense
CNO	Chief of Naval Operations
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COCOM	Combatant Commands
COGCON	Continuity of Government Readiness Condition
COLNAV	Columbian Navy
COMDTINST	Commandant Instruction
COMMCEN	Communication Center
COMMGRDLST	Command Guard List
COMMSHIFT	Communication Guard Shift
COMMSTA	Communication Station
COMMSYS	Communication System
COMNETWARCOM	Commander Naval Network Warfare Command
COMNAVSECGRU	Commander Naval Security Group Command
COMSATCOM	Commercial Satellite Communication
COMSEC	Communication Security
COMSPOT	Communication Spot
COMTAC	Communications Tactical
COOP	Continuity of Operations
COP	Common Operational Picture
COSPAS-SARSAT	Cosmicheskaya Sistyema Poiska Avariynich Sudov - Search and Rescue Satellite-Aided Tracking
COTHEN	Cellular over the Horizon Enforcement Network
COTR	Contracting Officers Technical Representative
CRF	Crypto Repair Facility
CSN	Communication Systems Network
CSO	Command Security Officer
CUDIXS	Common User Digital Information Exchange System

--- (D) ---

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
DES	Data Encryption Standard
DF	Direction Finding
DGPS	Differential Global Positioning System
DHS	Department of Homeland Security

DISA	Defense Information Systems Agency
DISCUS	Defense Satellite Communications System
DISN	Defense Information System Network
DITCO	Defense Information Technology Contracting Organization
DMS	Defense Messaging System
DNI	Director of National Intelligence
DOD	Department of Defense
DON	Department of Navy
DPRI	Directives, Publications and Reports Index
DPVS	Diversified PLA Verification System
DRS	Disaster Recovery System
DSC	Digital Selective Calling
DSL	Digital Subscriber Line
DSN	Defense Switch Network
DTG	Date-Time Group
DVL	Digital Voice Logger

--- (E) ---

EAIS	Encrypted Automatic Identification System
EEFI	Essential Elements of Friendly Information
E F T O	Encrypt for Transmission Only
EGC	Enhanced Group Call
EHF	Extremely High Frequency
E-MICP	Enhanced Mobile Incident Command Post
EMSS	Enhanced Mobile Satellite Service
EKMS	Electronic Key Management System
ELMER	Enterprise Land Mobile Radio
ELT	Emergency Locator Transmitter
E-Mail	Electronic Mail
EMCON	Emission Control
EMF	Enterprise Management Facility
EMSEC	Emission Security
EO	Executive Order
EPIRB	Emergency Position-Indicating Radio Beacon
ESB	Electronic Status Board
ESD	Electronic Support Detachment
ESU	Electronics Support Unit
EW	Electronic Warfare

--- (F) ---

FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FAX	Facsimile
FCC	Federal Communications Commission

FEC	Forward Error Correction
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FLS	Fleet Logistics System
FLTSAT	Fleet Satellite Communication System
FMR	Federal Management Regulation
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FRC	Federal Records Center
FRS	Family Radio Service
FSB	Fleet Satellite Broadcast
FSM	Fleet SIPRNET Messaging
FSS	Fixed Satellite Service
FST	Field Service Technician
FTS	Federal Telephone Service
FWTS	Federal Wireless Telecommunications Services

--- (G) ---

GANTSEC	Greater Antilles Section
GENADMIN	General Administrative
GENSER	General Service
GETS	Government Emergency Telecommunications Service
GFE	Government Furnished Equipment
GMDSS	Global Maritime Distress and Safety System
GMRS	General Mobile Radio Service
GOTHAM	Geo-Spatial over the Horizon ALE Matrix
GPS	Global Positioning System
GRT	Gross Registered Tons
GSA	General Services Administration
GSM-SM	Global System for Mobile Communication Security Module
GSSC	Global Satellite Communication Support Center

--- (H) ---

HF	High Frequency
HF-ALE	High Frequency-Automatic Link Establishment
HFDX	High Frequency Data Exchange
HIPA	Health Information Privacy Act
HLS Net	Homeland Security Network
HSPD	Homeland Security Presidential Directive
HYDROLANT	Navigational Warning covering eastern Atlantic Ocean and portion of the Arctic navigable waters.
HYDROPAC	Navigational Warning covering western Pacific Ocean, and Antarctic and portion of Arctic navigable waters.

--- (I) ---

IA	Information Assurance
IALA	International Association of Marine Aids to Navigation and Lighthouse Authorities
IAMSAR	International Aeronautical and Maritime Search and Rescue Manual
ICAO	International Civil Aviation Organization
ICE	Imaging and Communications Environment
ID	Identification
ID3	International Direct Distance Dialing
IEC	International Electrotechnical Commission
IMO	International Maritime Organization
IMPAC	International Merchant Purchase Authorization Card
INFO	Information Addressee, Record Message Prosign
INFOSEC	Information Security
INTEL	Intelligence
INTERCO	International Code of Signals
IP	Internet Protocol
IRR	International Radio Regulations
ISDN	Integrated Services Digital Network
ISIC	Immediate-Superior-In-Command
ISM	Iridium Security Module
ISSO	Information System Security Officer
ITU	International Telecommunications Union
IW	Integrated Waveform
IWN	Integrated Wireless Network

--- (J) ---

JAG	Judge Advocate General
JANAP	Joint Army, Navy, Air Force Publication
JIACC	Joint Inter-agency Counterdrug COMSEC
JIATF	Joint Interagency Task Force
JRS	Joint Reporting System
JSIR	Joint Spectrum Interference Report
JSP	Joint Satellite Panel
JTRS	Joint Tactical Radio System
JWICS	Joint Worldwide Intelligence Communications System

--- (K) ---

KBPS	Kilobits Per Second
KEYMAT	Keying Material
KMF	Key Management Facility
KMI	Key Management Infrastructure
KP	Key Processor

--- (L) ---

LAN	Local Area Network
LANTAREA	Atlantic Area
LANTCOMMSYS	Atlantic Area Communication System
LATA	Local Access and Transport Area
LCMS	Local COMSEC Management System
LEASAT	Leased Satellite
LE Sensitive	Law Enforcement Sensitive
LMD	Local Management Device
LOB	Line of Bearing
LRIT	Long Range Identification and Tracking

--- (M) ---

MARSEC	Marianas Section
MCC	Mobile Command Center
MCV	Mobile Command Vehicle
MDT	Message Distribution Terminal
MEDEVAC	Medical Evacuation
MEDICO	Medical Communications
MF	Medium Frequency
MHZ	Megahertz
MIB	Marine Information Broadcasts
MIFC	Maritime Intelligence Fusion Centers
MILSATCOM	Military Satellite Communication
MILSTAR	Military Strategic & Tactical Relay Satellite System
MINIMIZE	Term used to describe an Operational Condition declared by Command Authorities to clear military circuits of all non-essential telecommunication traffic in an actual, simulated or anticipated emergency.
MIOC	Maritime Information Operations Center
MISLE	Marine Information for Safety and Law Enforcement
MMSI	Maritime Mobile Service Identity
MOVREP	Movement Report
MPLS	Multi-Protocol Label Switching
MRC	Monthly Recurring Charge
MSI	Maritime Safety Information

MSS	Mobile Satellite Service
MUOS	Mobile User Objective System

--- (N) ---

NAFA	Non-Appropriated Funds Activity
NAIS	National Automatic Identification System
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NAVAREA	Navigational Area - Navigational Warning covering western Atlantic Ocean (NAVAREA IV), and eastern Pacific Ocean, eastern Bearing Sea and portion of Arctic Ocean (NAVAREA XII).
NAVCEN	Coast Guard Navigation Systems Center
NAVTEX	Navigational Telex. An international automated direct-printing service for delivery of navigational and meteorological warnings and forecasts, as well as urgent marine safety information to ships.
NAVMACS II	Naval Modular Automated Communications System (version 2)
NBDP	Narrow-Band Direct-Printing
NCA	National Command Authority
NCMS	Naval Communication Security Material System
NCS	National Communications System
NCTAMS	Naval Computer and Telecommunications Area Master Station
NDRS	National Distress and Response System
NEC	National Electrical Code
NECN	National Emergency Communications Network
NECOS	Net Control Station
NFPA	National Fire Protection Association
NGA	National Geospatial-Intelligence Agency
NIMS	National Incident Management System
NIPRNET	Non-Classified Internet Protocol Router Network
NIS	Navigation Information Service
NIST	National Institute of Standards and Technology
NLECC	National Law Enforcement Communications Center
NOAA	National Oceanic and Atmospheric Administration
NOC	Network Operations Center
NOFORN	Not Releasable to Foreign Nationals
NORTHCOM	United States Northern Command
NOTAL	Not to All Addressees
NRC	Non-Recurring Charge
NSA	National Security Agency
NSDD	National Security Decision Directives
NSEP	National Security Emergency Preparedness

NSI	National Security Information
NSS	National Search and Rescue Supplement
NSSPD	National Security Systems Policy Directive
NTIA	National Telecommunications and Information Administration
NTISSD	National Telecommunications and Information Systems Security Directive
NTM	Notice to Mariners
NTOC	National Threat Operations Center
NTP	Naval Telecommunications Procedures
NWP	Naval Warfare Publications
NWS	National Weather Service

--- (O) ---

OFCO	Operating Facility Change Order
OMB	Office of Management and Budget
ONS	Operational Needs Statement
OOD	Officer of the Deck
OPCON	Operational Control
OPFAC	Operating Facilities
OPLAN	Operations Plan
OPNAVINST	Office of the Chief of Naval Operations Instructions
OPORDER	Operational Order
OPSEC	Operations Security
OPS NORMAL	Operations Normal
OPTASK	Operational Tasking
ORD	Operational Requirements Document
OS	Operations Specialist
OSC	Coast Guard Operations System Center
OSHA	Occupational Safety and Health Act
OTAR	Over the Air Rekeying
OTC	Officer In Tactical Command

--- (P) ---

PACAREA	Pacific Area
PACCOMMSYS	Pacific Area Communication System
PAL	Personnel Allowance List
PATFORSWA	Patrol Forces Southwest Asia
PBX	Private Branch Exchange
PC	Personal Computer
PCII	Protected Critical Infrastructure Information
PDC	Program Designator Codes
PERSEC	Personnel Security
PHYSEC	Physical Security

PII	Personal Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLA	Plain Language Address
PLB	Personal Locator Beacon
PO	Post Office
POC	Point of Contact
PROFORMA	Pre Formatted Record Message
PSTN	Public Switched Telephone Network

--- (R) ---

R&D	Research and Development
R21	Rescue 21
RADIOFAX	Radio Facsimile
RADLOGS	Radio Logs
RAM	Random Access Memory
RCC	Rescue Coordination Center
RF	Radio Frequency
RFF	Remote Fixed Facility
RFS	Request for Service
RMKS	Remarks, Record Message Prosign
RPC	Regional Planning Committee
RQI	Received Quality Indication
RSC	Rescue Sub-Center
RSSI	Received Signal Strength Indication

--- (S) ---

SAC	Service Access Codes
SAG	Secure Air to Ground
SAR	Search and Rescue
SARSAT	Search and Rescue Satellite Aided Tracking
SART	Search and Rescue radar Transponder
SATCOM	Satellite Communication
SATHICOM	Satellite High Command
SBU	Sensitive But Unclassified
SCC	Sector Command Center
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDB	Satellite Database
SDLC	System Development Life Cycle
SDS	Satellite Data System
SDX	Satellite Data Exchange
SECDEF	Secretary of Defense
SECDHS	Secretary, Department of Homeland Security

SECNAV	Secretary of Navy
SEF	Special Category Exclusive For
SFLC	Surface Forces Logistics Command
SHARES	Shared Resources
SHD	Special Handling Designator
SHF	Super High Frequency
SIM	Subscriber Identity Module
SIOP-ESI	Single Integrated Operational Plan-Extremely Sensitive Information
SIPRCHAT	Secret Internet Protocol Router Network Chat
SIPRNET	Secret Internet Protocol Router Network
SITOR	Simplex Teletype over Radio
SMC	SAR Mission Coordinator
SMEF	System Management and Engineering Facility
SOLAS	Safety of Life at Sea
SOP	Standard Operating Procedure
SORTS	Status of Resources and Training System
SOSO	Speed of Service Objective
SPAWAR	Space and Naval Warfare Systems
SPECAT	Special Category
SPII	Sensitive Personal Identifiable Information
SRU	Search and Rescue Unit
SSA	Systems Support Agent
SSIC	Standard Subject Indicator Code
STE	Secure Telephone Equipment
SUBJ	Subject, Record Message Prosign
SURPIC	Surface Picture
SVN	Secure Voice Network

--- (T) ---

TACON	Tactical Control
TACT	Tailored Annual Cutter Training
TASK	Task Organization
TBA	Terminal Base Address
TCC	Transportable Communication Central
TCO	Telecommunications Certification Office
TCP/IP	Transmission Control Protocol/Internet Protocol
TCTO	Time Compliance Technical Order
TEMPEST	A term used to describe Electronic Countermeasure policy and requirements
TIN	Tactical Information Network
TIC	Trusted Internet Connection
TISCOM	Telecommunication and Information Systems Command
TO	Action Addressee, Record Message Prosign
TOR	Time of Receipt

TRANSEC	Transmission Security
TS	Top Secret
TSP	Telecommunication Service Priority
TSTA	Tailored Ships Training Availability
TTP	Tactics, Techniques and Procedures
TWA	Time Weighted Average

--- (U) ---

UC	Unified Communications
UFO	UHF Follow on
UHF	Ultra High Frequency
UHF-FM	Ultra High Frequency – Frequency Modulated
UMIB	Urgent Marine Information Broadcast
UNCLAS	Unclassified, Security Classification
UNCLOG	U.S. Coast Guard / National Weather Service Coordination-Liaison Working Group
UPS	Uninterruptible Power Supply
U.S.C.	United States Code
USMTF	United States Message Text Format
USN	United States Navy
USNDA	United States National Distribution Authority
USSTRATCOM	Commander, United States Strategic Command
UTC	Coordinated Universal Time

--- (V) ---

VDLS	Vaults, Depot, and Logistics System
VHF	Very High Frequency
VHF-FM	Very High Frequency – Frequency Modulated
VOBRA	Voice Broadcast Automation
VoIP	Voice over Internet Protocol
VSWR	Voltage Standing Wave Ratio
VTC	Video Teleconferencing
VTS	Vessel Traffic Service

--- (W) ---

WAGB	Coast Guard Icebreaker
WAN	Wide Area Network
WHEC	Coast Guard High Endurance Cutter
WIX	Coast Guard Training Cutter Eagle
WITS	Washington Interagency Telecommunications System
WLB	Coast Guard Buoy Tender, Seagoing
WLM	Coast Guard Buoy Tender, Coastal
WMEC	Coast Guard Medium Endurance Cutter

WMSL	Coast Guard Maritime Security Cutter, Large
WPB	Coast Guard Patrol Boat
WPS	Wireless Priority Service
WTGB	Coast Guard Icebreaker Tug

--- (X) ---

XMT	Exempt Addressee

Index

8

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X

COMDTINST M2000.3E