U.S. Department of
Homeland Security

United States
Coast Guard

TELECOMMUNICATION MANUAL

COMDTINST M2000.3F
April 2013

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 M2000.3F

APR 19, 2013

COMMANDANT INSTRUCTION M2000.3F

Subj: TELECOMMUNICATION MANUAL

Ref:
(a) Telecommunication Tactics, Techniques, and Procedures, CGTTP 6-01.2 (series)
(b) United States Coast Guard Regulations 1992, COMDTINST M5000.3 (series)
(c) U.S. Coast Guard Addendum to the United States National Search and Rescue Supplement (NSS) to the International Aeronautical and Maritime Search and Rescue Manual (IAMSAR), COMDTINST M16130.2 (series)
(d) U.S Navy - U.S. Coast Guard Communications Policy, OPNAVINST 2000.20D (series)/COMDTINST 2000.9 (series)
(e) Directives, Publications and Reports Index (DPRI), COMDTNOTE 5600
(f) COMTAC Publication Policy and Procedures Manual, COMDTINST M2600.1 (series)
(g) CMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3, EKMS 1 (series)
(h) Spectrum Management Policy and Procedures, COMDTINST M2400.1 (series)
(i) Electronics Manual, COMDTINST M10550.25 (series)
(j) U.S. Coast Guard Security and Information Assurance Manual, COMDTINST 5500.13 (series)
(k) Limited Personal Use of Government Office Equipment and Services, COMDTINST 5375.1 (series)
(l) Satellite Communications, CJCSI 6250.1 (series)
(m) U.S. Coast Guard TEMPEST Program, COMDTINST M2241.6 (series)
(n) Classified Information Management Program, COMDTINST M5510.23 (series)
(o) Naval Operational Planning, NWP 5-01 (series)
(p) Naval Communications, NTP 4 (series)
(q) Personnel Security and Suitability Program, COMDTINST M5520.12 (series)
(r) Physical Security and Force Protection Program, COMDTINST M5530.1 (series)
(s) Communication Security (COMSEC), National Telecommunications and Information

DISTRIBUTION – SDL No. 162

	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

Systems Security Directive Number 600 (NTISSD No. 600)
(t) Electronic Key Management System (EKMS Inspection Manual), EKMS 3 (series)
(u) Information and Life Cycle Management Manual, COMDTINST M5212.12 (series)
(v) Civil Engineering Manual, COMDTINST M11000.11 (series)
(w) Communications Instructions Signaling Procedures in the Visual Medium, ACP 130 (series)
(x) Radiotelephone Handbook, CGTTP 6-01.1 (series)
(y) Aids to Navigation Manual – Administration, COMDTINST M16500.7 (series)

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

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

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

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

   a. Tactics, techniques, and procedures (TTP) were extracted from this Manual and promulgated in Telecommunication TTP, CGTTP 6-01.2. This Manual was restructured to improve the flow of information after TTP extraction.

   b. Removal of 2182 kHz distress watchkeeping requirements.

   c. Inclusion of Health Insurance Portability and Accountability Act of 1996 (HIPAA) information as it relates to communications.

   d. Inclusion of Contingency Communications Plan (CCP) policy.

   e. Incorporated a separate Chapter for Coast Guard Auxiliary telecommunication.

   f. The term Marine Information Broadcast (MIB) replaced with Broadcast Notice to Mariner (BNM) to align with the Code of Federal Regulations (C.F.R.), International Telecommunications Union (ITU) Regulations, and CG aids to navigation terminology.

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

      004/11: Encrypted Automatic Identification System (EAIS) Keyset Distribution to Port Partners and other Government Agencies (Chapter 5)
      012/11: Reporting Loss of Tactical Radio or Key Variable Loader (Chapter 5)
      005/12: Release Authority of ALCOAST Messages (Chapter 13)
      009/12: Standard Aviation Wulfberg RT-5000 VHF/UHF Code Plugs (Chapter 4)

010/12: Format Change to Coast Guard Record Messages (Chapter 13)
011/12: Operations Security for Rescue 21 Mixed Mode Patched Circuits (Chapter 4)
012/12: Use of Office Codes in Coast Guard Record Messages (Chapter 13)
013/12: Recorded Tactical Voice Communications Retention (Chapter 4)
014/12: NAIS AIS Message Transmission (Chapter 3)

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 in itself a rule. It is intended to provide guidance for Coast Guard personnel and is not intended to nor does it impose legally-binding requirements on any party outside the Coast Guard.

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). This policy does not have any significant or substantial change to existing records management requirements.

8. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.

   a. The development of this directive and the general policies contained within it have been thoroughly reviewed by the originating office and are categorically excluded under current USCG categorical exclusion (CE) #33 from further environmental analysis, in accordance with section 2.B.2. and Figure 2-1 of the National Environmental Policy Act Implementing Procedures and Policy for Considering Environmental Impacts, COMDTINST M16475.1 (series).

   b. This directive will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policies in this Manual must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), Council on Environmental Policy NEPA regulations at 40 CFR Parts 1500-1508, DHS and Coast Guard NEPA policy, and compliance with all other environmental mandates.

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/
Rear Admiral, U.S. Coast Guard
Chief Information Officer

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

TABLE OF CONTENTS

CHAPTER 1 COAST GUARD (CG) TELECOMMUNICATION ORGANIZATION

A. General. As specified in Telecommunications Operations, 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 Coast Guard Telecommunication System (CGTS) is an essential resource under DHS, providing the means to share mission critical information with other DHS agencies, the Department of Defense (DOD) and federal, state, local, and tribal law enforcement officials to meet the objectives of defending our nation.

B. Coast Guard Telecommunication System (CGTS).

1. Definition. The CGTS links United States Coast Guard (CG) assets (e.g., shore units, aircraft, cutters, and boats) to other agencies and organizations throughout the nation and world. It encompasses all radio, satellite, telephone, and network facilities owned/leased, controlled, and 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 or protected, and interoperable telecommunications to meet Coast Guard operational requirements.

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

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

C. Coast Guard Telecommunication System (CGTS) Program Management Roles and Responsibilities. Program management of the CGTS is a CG headquarters responsibility. It involves the planning, programming, and budgeting for CGTS along with national and international representation of CG interest. The following section is a list of roles and responsibilities as related to the CGTS.

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 Policy Management. Communications policy management and publication is within the Office of Information Assurance and Spectrum Policy (CG-65).

4. Information Assurance (IA) and Communication Security (COMSEC). IA and COMSEC are the responsibility of the Office of Information Assurance and Spectrum Policy (CG-65).

5. Spectrum Management. Spectrum management is the responsibility of the Office of Information Assurance and Spectrum Policy (CG-65).

6. Communications Asset Management. Management oversight of deployed systems is the responsibility of the Office of Enterprise Infrastructure Management (CG-64).

7. Communications Doctrine, Tactics, Techniques and Procedures (TTP). The area command, control, communication, computers, and information technology (C4IT) divisions are responsible for the development and dissemination of communication doctrine, to include operational communication planning. Commander, Forces Training Command (FORCECOM) facilitates the development and dissemination of telecommunication TTP.

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. Coast Guard Telecommunication System (CGTS) 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 telecommunication systems are appropriately engineered, acquired, and maintained throughout the full system life-cycle. These organizations and the relationship to the CGTS are discussed in sections E and F of this Chapter.

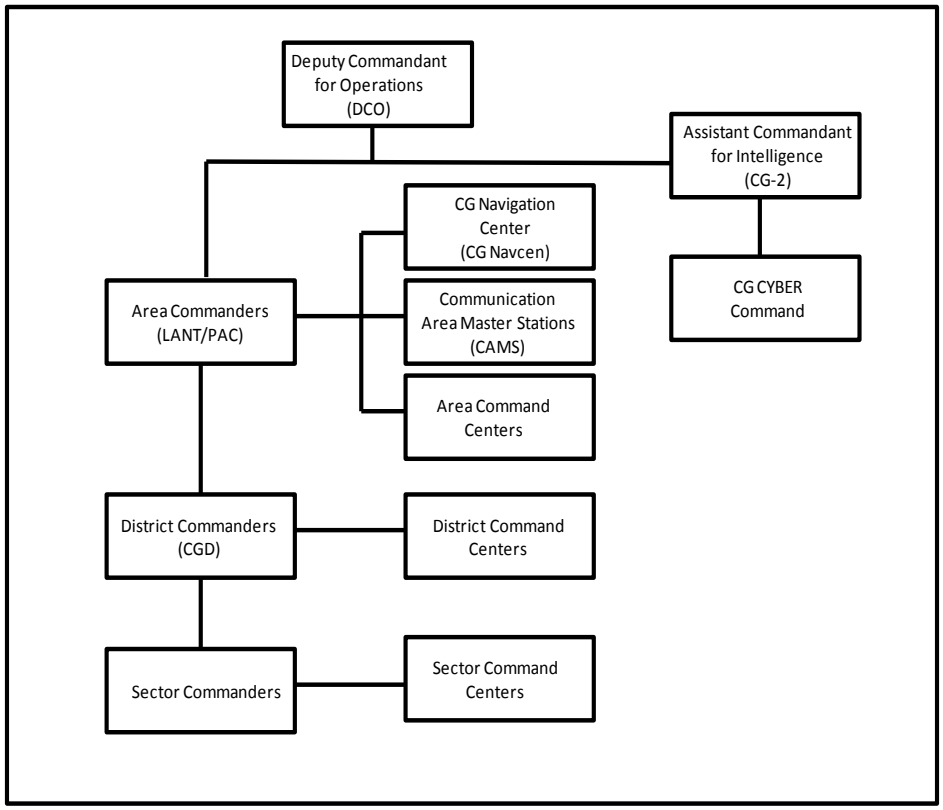
E. Deputy Commandant for Mission Operations (DCO).

1. CGTS Command and Control Organizational Hierarchy. Command and control of the CGTS is exercised per Reference (b), relative to rank and command. Exhibit 1-1 illustrates the CGTS command and control hierarchy.

2. CG Cyber Command. The CG Cyber Command serves as the CG component to United States Cyber Command. The mission of the CG Cyber Command 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, and support DHS cyber missions. The CG Cyber Command coordinates CG enterprise network response through the TISCOM IT Operations Center (ITOC) (see

Telecommunication and Information Systems Command (TISCOM) in section F.4.a.(1) of this Chapter).

Exhibit 1-1
CGTS Command and Control Organizational Hierarchy



3. Area Commanders. Area commanders shall exercise administrative control (ADCON) and operational control (OPCON) of the communication system (COMMSYS), less the CG One Network (CGOne), within their geographic area of responsibility (AOR). 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). Additional area responsibility is described in the following section, including a list of facilities within the area COMMSYS.

   a. The Atlantic Area (LANTAREA) Chief, C4IT and Security Division (LANT-6) and Pacific Area (PACAREA) Chief, C4IT and Security Division (PAC-6) are responsible for exercising OPCON and ADCON of the Atlantic Area

communication system (LANTCOMMSYS) and the Pacific Area communication system (PACCOMMSYS) respectively. This includes communication area master stations (CAMS), subordinate communication stations (COMMSTA), mobile command centers (MCC), contingency communications caches, and the Rescue 21 (R21) Disaster Recovery System (DRS). Additional responsibilities include operational and administrative oversight of area and district COMSEC, IA, information security (INFOSEC), personnel security (PERSEC) and physical security programs. The Coast Guard (CG) Navigation Center (NAVCEN) is under ADCON and OPCON of LANTAREA.

b. Area commanders can delegate authority to the 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. The area COMMSYS is subcategorized into the following facilities and services:

(1) Communication Area Master Station (CAMS). CAMS are the area master telecommunication station providing rapid, reliable, secure or protected, and interoperable communication support to CG operational commanders and other government agencies. See Chapter 7 of this Manual for additional information on CAMS operations. The following section describes services provided by the CAMS to support the area commander.

(a) Communications Assist Team (CAT). CAT training and support services are available to cutters and other units as directed by the area commander within their geographic AOR.

(b) Contingency Communications Caches. The CAMS operate and maintain an inventory of MCCs and portable communications assets. These assets are 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.

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

4. District Commanders. The Chief, Telecommunications Division/Branch, shall serve as the single point of coordination for establishing operational requirements for CG telecommunications within the district AOR. The Chief, Telecommunications Division/Branch, under the direction of the district commander, shall provide telecommunication services for the district office, as well as, exercise OPCON and ADCON of the CGTS within the district geographic AOR, unless otherwise directed by the area commander. The district command center (CC) provides command and control of operations and assets within its jurisdiction.

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) is the integrator for all operations within a sector's AOR and the communications unit is the hub for all voice and data communications.

6. Communications Officer/Communications Supervisor. A communications officer or communications supervisor shall be designated in writing 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 communication of the command. 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. Further information on these duties are prescribed as follows:

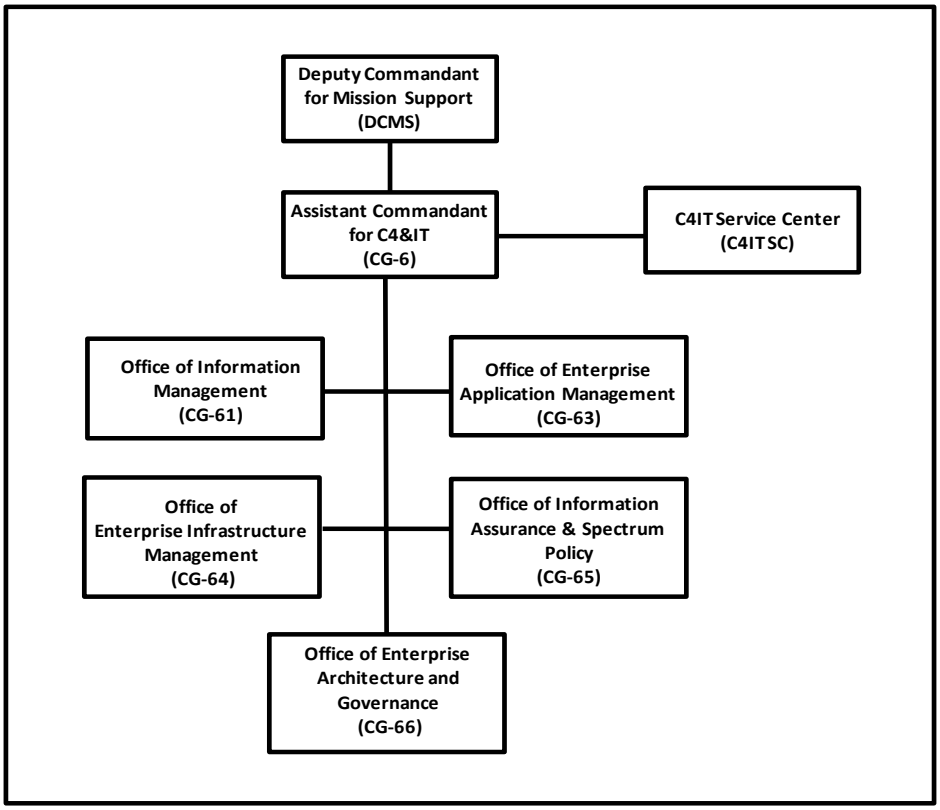
   a. Communications Officer: See Reference (b).

   b. Communications Supervisor: U.S. Coast Guard Sector Organization Manual, COMDTINST M5401.6 (series).

F. Deputy Commandant for Mission Support (DCMS). The following section describes the Commandant (CG-6) structure, shown in Exhibit 1-2, as it supports the CGTS.

1. Assistant Commandant for C4&IT (CG-6). The mission of Commandant (CG-6) is to enhance C4IT's value in the performance of CG missions by developing and aligning enterprise strategies, policies, and resource decisions with the CG strategic goals, mandates, and customer requirements. Specific roles and responsibilities associated with Commandant (CG-6) are per Command, Control, Communications, Computers, and Information Technology (C4&IT) Investment Management Policy, COMDTINST 5230.71 (series).

Exhibit 1-2
Commandant (CG-6) Organization



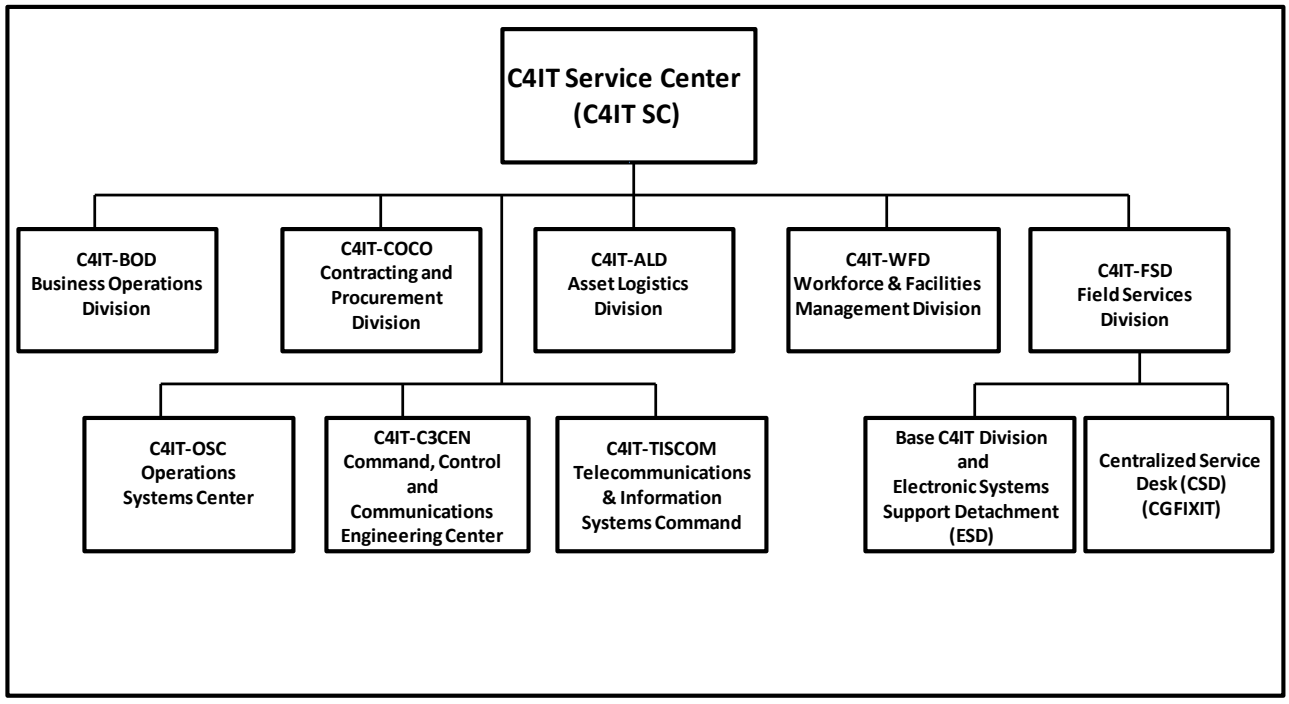
2. Office of Information Assurance (IA) and Spectrum Policy (CG 65). Commandant (CG-65) serves as program manager for the CGTS. Responsibilities include promoting and protecting all C4IT infrastructure and its associated information through the development and integration of effective defense-in-depth security strategies, technologies, policies, controls, and standards that ensures the reliability and availability of the CG's C4IT enterprise infrastructure in enabling successful mission execution. Additionally, this office aligns security and IA oversight in the execution of the CG's telecommunication program through effective planning, evaluation, and adoption of telecommunication technology standards, and creation and enforcement of telecommunication policy.

3. Office of Enterprise Infrastructure Management (CG-64). Commandant (CG-64) establishes policy and performs centralized management of all phases of the system development life-cycle for C4IT infrastructure CG-wide. This office serves as the customer interface for introduction of all new business requirements validated by

Commandant (CG-761). Additionally, Commandant (CG-64) manages enterprise architecture coordination and provides oversight for the design, development, and acquisition of new infrastructure systems, in addition to, the operations, maintenance, and enhancement of legacy systems.

4. Command, Control, Communications, Computers, and Information Technology Service Center (C4IT SC). The mission of the C4IT SC is to provide full life-cycle support for CG C4IT applications, systems, and infrastructure. The C4IT SC organization hierarchy is shown in Exhibit 1-3, with further information in the following section.

Exhibit 1-3
C4IT SC Organizational Hierarchy



a. C4IT SC oversees the operation of the three C4IT centers of excellence: OSC, TISCOM and C3CEN. The following section describes the functions of each.

(1) Operations Systems 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, and Communications Engineering Center (C3CEN). C3CEN develops, builds, fields, and supports advanced electronic command, control, communication, and navigation systems derived from operational requirements from DCO. C3CEN facilitates evolutionary engineering that focuses on the rapid deployment of essential functionality followed by planned improvements based on enhanced or refined requirements. C3CENs product lines include CAMS, subordinate COMMSTAs, MCCs, contingency communication cashes, and the DRS.

(3) Telecommunication and Information Systems Command (TISCOM). TISCOM provides full life-cycle support for enterprise information systems infrastructure and associated networking infrastructure through the cohesive alignment of two product lines (Enterprise Information Systems Infrastructure and Enterprise Network Infrastructure). Within these product lines, TISCOM develops, fields, maintains, and provides user support to improve CG mission performance through the innovative use of applications and networking technology. As an extension of these two product lines, TISCOM Enterprise Systems Operations Division, provides a 24/7 watch and maintains the CG's ITOC, providing enterprise information systems infrastructure management and enterprise network management.

b. Under field support delivery elements, the electronic systems support is provided by the regional base C4IT division and the respective electronic systems support detachments (ESD) provide units with C4IT maintenance and casualty response.

Note: Electronic Systems Support Units (ESU) are now base C4IT divisions.

G. Coast Guard Telecommunication System (CGTS) Relationship to Other Organizations. 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 can communicate and remain interoperable with the CG, DHS and the Continuity Communications Managers Group. The following sections outline some of the other organizations that support the CGTS.

1. Department of Homeland Security Office of Emergency Communications (OEC). Established by Congress in 2007 in response to communications challenges witnessed

during the attacks on September 11, 2001 and during Hurricane Katrina, the Department of Homeland Security (DHS) Office of Emergency Communications (OEC) partners with emergency communications personnel and government officials at all levels of government to lead the nationwide effort to improve emergency communications capabilities. On July 6, 2012, Executive Order 13618 was issued to update and clarify national security and emergency preparedness (NS/EP) communications responsibilities for the Federal government. As a result, DHS realigned programs within OEC and the former National Communications System (NCS) to lead the Department's support for emergency communications and NS/EP communications programs.

a. The combined services of OEC's traditional support for interoperable communications along with the former NCS' technical capabilities for NS/EP communications resulted in a comprehensive office to address all emergency communications issues.

b. The CG participates in OEC activities and programs such as the Shared Resources (SHARES) High Frequency Radio Program and the National Emergency Communications Network (NECN). The SHARES and NECN programs function under the DHS Office of Cybersecurity and Communications when activated.

c. Further information on the Presidential Directive which claims power to execute procedures for continuity of the federal government in the event of a "catastrophic emergency" is in National Security and Homeland Security Presidential Directive NSPD 51/HSPD 20.

2. Defense Communications System (DCS). The Defense Information Systems Agency (DISA) exercises OPCON 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 C4IT SC is the principal agent for the CG.

3. Federal Communications Commission (FCC). The FCC was created by the Communications Act of 1934 and is charged with regulating interstate and international communication by radio, television, wire, satellite, and cable. The FCC furnishes radio direction finding services when requested for search and rescue (SAR) and harmful interference cases. CG units are authorized and encouraged to coordinate with the FCC at the local level.

CHAPTER 2 COAST GUARD (CG) TELECOMMUNICATION GOVERNANCE AND POLICIES

A. General. This Chapter provides the national and federal governance that allows the CG to operate telecommunication services, guidance for telecommunication publication libraries, and telecommunication policies.

B. Governance.

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

   a. Establish, install, abandon, re-establish, reroute, operate, maintain, repair, purchase, or lease such telephone and cables, together with all facilities, apparatus, equipment, structures, appurtenances, accessories, and supplies used or useful in connection with the installation, operation, maintenance, or repair of such lines and cables, including telephones in residences leased or owned by the government of the United States when appropriate to assure efficient response to extraordinary operational contingencies of a limited duration, and acquire such real property rights of way, easements, or attachment privileges as may be required for the installation, operation, and maintenance of such lines, cables, and equipment (14 United States Code (U.S.C.) § 93(a)(15));

   b. Establish, install, abandon, re-establish, change the location of, operate, maintain, and repair radio transmitting and receiving stations (14 U.S.C. § 93(a)(16)); and

   c. 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).

2. Commandant (CG-6) supports all CG missions through timely delivery of telecommunication and information technology services. For telecommunications, CG operational and administrative communication 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. Memorandum of Agreement (MOA) and Memorandum of Understanding (MOU) with other federal, state, local, and tribal agencies.

3. In the United States, maritime services are promulgated under the Communications Act of 1934, as amended (47 U.S.C. § 151 et seq.), and the rules and regulations implementing the act adopted by the FCC in 47 Code of Federal Regulations (C.F.R.) §

151. Part 80 of the C.F.R. governs public stations in the Maritime Services, 47 C.F.R. These communications are regulated by two entities:

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

b. The NTIA regulates federal use of the spectrum by authority granted in the Communications Act of 1934 at 47 U.S.C. § 305, through The Manual of Regulations and Procedures for Federal Radio Frequency Management.

4. Both federal and public requirements are an integral part of the CGTS. While the CG's internal use of the radio spectrum is regulated by NTIA, FCC requirements placed on public users of the spectrum have a direct and significant impact on CG operations. There are numerous requirements imposed on the CG operation of communication facilities, in addition to the requirements of the Communications Act of 1934, the NTIA, 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 Global Maritime Distress and Safety System (GMDSS)); and

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

(2) Volume 2: Appendices;

(3) Volume 3: Resolutions and Recommendations; and

(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);

e. Commercial Fishing Industry Vessel Safety Act of 1988, as amended (46 U.S.C. § 2101 et seq: 46 U.S.C. §§ 4501-4508 – Applicability to certain fishing vessels);

f. 1963 Presidential Decision establishing National Communications System (NCS) –

High Frequency (HF) Nets. Now under EO 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions;

g. Allied Communication Publications (ACP), Joint Army, Navy, Air Force Publications (JANAP), Naval Telecommunications Procedures (NTP), and Naval Warfare Publications (NWP);

h. Management of Domestic Incidents – DHS/DOD Interoperability, Homeland Security Presidential Directive 5;

i. DHS National Emergency Communications Plan – DHS Interoperability;

j. Department of Homeland Security National Security Systems Policy Directives, DHS NSSPD 4300 (series);

k. Operations Security Program, Department of Homeland Security Management Directive System MD Number 11060.1; and

l. This Manual, References (c) and (d), various IA, COMSEC, operations security (OPSEC), and PERSEC policies and directives concerning the security of communications, including, but not limited to, National Security Decision Directives and Committee on National Security Systems policies.

C. Telecommunication Library. All units using CG record messaging services 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 shall maintain either paper copies or local electronic versions retrievable from onboard computers or stored off line on compact discs. At a minimum, the following publications are required:

1. This Manual;

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

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

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

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

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

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

8. Naval Communications, NTP 4 (series);

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

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

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

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

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

D. General Telecommunication Policies. CG telecommunications shall be conducted per this Manual, federal requirements and policies, International Radio Regulations (IRR), treaties and international agreements, joint and allied/combined communication instructions, NTPs, Commandant instructions (COMDTINST), area and district publications, and directives issued by appropriate authority. The various communication and COMSEC publications are provided as follows:

1. Communication publications are distributed to the appropriate CG commands per Reference (e) and (f); and

2. COMSEC publications are issued by the United States National Distribution Authority per Reference (g).

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

1. Interagency 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. Reference (d) 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 per the Privacy Act of 1974, 5 U.S.C. § 552a. Inviolability, in this case, means that no personally identifiable information (PII) (including PII in organization record messages, electronic mail (email), and/or via voice) may be released or divulged beyond the recipients intended by

the originator of the information. Express consent from the originator is required for further dissemination of PII.

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

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

   b. CG members shall take precaution when transmitting patient health information, minimizing the chance of the incidental disclosures.

5. Delivery of Emergency Messages to Private Vessels. The CG has no authority to handle private communication between persons ashore and commercial or private vessels. The following policy applies:

   a. If a CG unit is asked to deliver a personal message to a vessel, the CG unit shall advise the requestor to file the message by commercial means; and

   b. The CG can relay a request to contact the marine operator for an emergency message to a vessel.

6. Release of Information Acquired from Telecommunication. The requirement and procedures for the CG to furnish information to the public is set forth in Reference (b), 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 Coast Guard (CG) Units. During a national emergency, natural disaster, or other significant events, CG units are authorized to broadcast public service information, provided the broadcast does not interfere with primary missions. Refer requests from the news media to Assistant Commandant for Governmental and Public Affairs (CG-092) for approval.

8. Release of Radio Direction Finder Bearings. Per Reference (c), the CG cannot assume responsibility for navigating a vessel, but it is authorized to provide the master of a vessel certain navigation information. Refer to Reference (c) for further guidance on what information can be provided.

9. Special Authorization for Use of Radio. Use of radio within the territorial waters of any nation falls under the jurisdiction of that nation, and therefore requires authorization for such operations.

10. 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 Foreign Port Calls, COMDTINST 3128.1 (series). The foreign

port clearance record message requires specific information regarding radio requirements of the command.

11. Use of Radio by Foreign Men-of-War in 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. The following policy applies:

    a. These ships shall observe the radio regulations currently in effect for the area in which they are operating;

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

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

12. Mission Support Policies. Information on mission support policies and procedures for CGTS is available through the Mission Support Handbook. The Mission Support Handbook is available on line at https://cgportal2.uscg.mil/units/dcms/dcms-mission-support-organization/SitePages/Home.aspx. Questions regarding information contained in the Mission Support Handbook can be directed to: AskMissionSupport@uscg.mil.

F. Telecommunication Policy Dissemination. 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 numbered policy record message issued in a new calendar year lists the previous year's policy record messages which remain in effect. Current telecommunications policy record messages and points of contact for telecommunications policy and issues can be found at: https://cgportal2.uscg.mil/units/cg652/SitePages/Home.aspx.

CHAPTER 3 COAST GUARD TELECOMMUNICATION SYSTEM (CGTS) INFRASTRUCTURE

A. General. The CGTS includes owned and leased circuits, channels, services, and equipment that provide data, voice, and video networks throughout the CG. This Chapter defines systems and details policies pertaining to radio systems, networks, telephony, and satellite communication services. See Chapter 4 of this Manual for CGTS procurement policy.

B. Oversight and Management Functions. The C4IT SC engineers, documents, and implements the CG telecommunication and information systems infrastructure. The following section outlines C4IT SC responsibilities for the CGTS.

1. The C4IT SC provides oversight for the following CG telephone, network, and commercial telecommunication services:

   a. Federal telephone services (FTS) contracts. The C4IT SC administers FTS contracts including: Networx and GSA telecommunication contracts such as Washington Interagency Telecommunications System 3 (WITS3), International Direct Distance Dialing 3 (ID3), Federal Wireless Telecommunications Services (FWTS), electronic commerce, internet access, email, etc;

   b. CGOne;

   c. All commercial satellite communication (COMSATCOM) services (e.g., Inmarsat fleet broadband, Ku-band) and associated contracts;

   d. Microwave services;

   e. 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, mobile and fixed satellite service, and Defense Switch Network (DSN);

   f. Any interagency service provided to CG units (e.g., National Weather Service (NWS)) for special organization-wide networks; and

   g. All data and voice system encryption devices.

2. The C4IT SC administers the telecommunications 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 per Use of Unclassified Wireless Devices, Services, and Technologies, COMDTINST

2010.2 (series); and

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

C. Radio Systems.

1. Rescue 21. Only unclassified or sensitive-but-unclassified (SBU) information shall be discussed when using the R21 interconnected intercom.

2. Participation in Federal, State, or Local Wireless Voice Networks. The following section outlines the policies and options for participation in wireless networks.

a. Whenever possible, units shall use a common frequency already authorized for both the CG and federal, state, and local partners. Marine band use shall be per Reference (h).

b. Any use of CG frequencies by non-government agencies shall be authorized in writing by Commandant (CG-65) and shall only be used for communication with CG assets.

c. CG use of public safety frequency license, particularly the public safety bands (700/800 MHz), must be certified as necessary in writing by local partners per Reference (h).

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

(1) Cutters. Installations shall be completed per Reference (i);

(2) Standard Boats. Installations shall be completed per Reference (i). Options in sections 4.a and 4.b of this Chapter and handheld radios (provided by other government agency or purchased) are authorized until a CG-wide solution for boats is identified;

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

(4) Shore Units. Installations shall be completed per Reference (i).

e. Connecting a CG radio communication asset (HF, very high frequency (VHF), ultra high frequency (UHF)) to a federal, state, or local agency's interoperability system (e.g., Integrated Wireless Network (IWN), Enterprise Land Mobile Radio (ELMR), 800 MHz, HF/VHF, trunked or conventional) is authorized. This connection can be made permanently or on an as-needed basis. Without the assurance of end-to-end encryption, circuits shall be considered unprotected.

f. Units shall notify their district spectrum manager, for further coordination with district telecommunications division/branch, prior to adding new frequencies to code plugs, authorizing additional users to current CG frequency authorizations, or using another agency's radio frequency.

g. Units shall notify Commandant (CG-65 and CG-64) and area C4IT division (LANT-6 or PAC-6) of federal, state, or local wireless voice network participation, procurement, and installation via their chain-of-command.

3. 800 Megahertz (MHz) Radios. The following policy applies for 800 MHz radios:

a. 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.

b. 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), and state or local government agency. There are 55 RPCs that have been established by the FCC which are responsible for coordinating interoperability for their region. Further information for RPCs and mutual-aid channels can be found at the following sites:

(1) Information on the RPCs: http://publicsafety.fcc.gov/pshs/public-safety-spectrum/800-MHz/rpc-directory.htm; and

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

c. The written formal MOA 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. Requests for use of 800 MHz radios shall be routed to the area C4IT and district telecommunications division/branch for approval. A copy of the signed interagency agreement shall be forwarded to Commandant (CG-652) to facilitate enterprise-wide agency coordination.

4. Other Radio Systems. Other operationally specific radio systems exist to meet the CG's requirement to serve the public interest or satisfy treaty requirements, to include but not

limited to, the National Distress and Response System (NDRS), R21, and Differential Global Positioning System (DGPS).

D. Data Networks. A data network is a group of interconnected (via cable and/or wireless) computers and peripherals that are capable of sharing software and hardware resources between many users. CG commands are connected through a wide variety of data networks that are public, unclassified, and secure. Data networks are administered and provisioned by the C4IT SC and serviced by the regional base C4IT division. The following section is a list of approved CG networks.

1. Department of Homeland Security One Network (DHS OneNet). DHS OneNet is the unclassified wide-area network (WAN) for DHS. DHS OneNet is a multi-protocol label switching (MPLS) network. MPLS is a standards-approved technology that speeds up network traffic flow and makes it easier to manage. DHS OneNet may be used to process SBU information.

2. Coast Guard One Network (CGOne). CGOne is the CG implementation of DHS OneNet. Additional information is as follows:

   a. CGOne provides CG units access to the internet; and

   b. TISCOM monitors the network on a 24/7 basis at the ITOC.

3. Internet. The internet is a publically accessible (non-secure) global system of interconnected computer networks. Refer to Reference (j) for additional policies and guidance on the installation and use of commercially provided internet services at CG facilities. All non-standard internet (not connected to CGOne) requests shall be ordered by the local designated agency representative (DAR) only (see Chapter 4 of this Manual for further DAR responsibilities).

4. Secret Internet Protocol Router Network (SIPRNET). SIPRNET is an enterprise-wide administered WAN capable of providing a secure infrastructure for the exchange of voice, video, data, and imagery. SIPRNET is cleared up to the Secret/Not Releasable to Foreign Nationals (Secret/NOFORN) classification level and can be used to process North Atlantic Treaty Organization (NATO) Secret and below information. Although SIPRNET operates similar to the internet, it is a DOD managed secure network limited to authorized United States government employees. The following section contains additional SIPRNET information.

   a. 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.

   b. Units shall submit requests for SIPRNET installation, de-installation, and support per Reference (a).

c. Refer to Secret Internet Protocol Router Network (SIPRNET) Management Policy, COMDTINST 2070.20 (series) for specific SIPRNET guidance.

5. 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.

6. Joint Worldwide Intelligence Communications System (JWICS). JWICS is an enterprise administered WAN link encrypted internet protocol (IP) network that operates at the Top Secret/Sensitive Compartmented Information (TS/SCI) level for data and video support throughout DOD and other federal agencies.

7. Other Networks. Other operationally specific networks exist to meet the CG's requirement to serve the public interest or satisfy treaty requirements. An example of such network is the Communication Systems Network (CSN).

E. Telephony. The following section describes CG telephony services.

1. Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS). See Reference (a) for GETS and WPS procedures. CG policy is to provide WPS for government provided cellular phones only.

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

a. 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;

b. Long distance access. Dedicated lines or central exchange access provided by General Services Administration (GSA) or the CG are preferred. If physical access is not available, federal calling cards can be used;

c. Continuous recorded monitoring of critical telephone circuits, as required, to document verbal agreements and pertinent information exchanges. Such recordings constitute permanent records that can 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; and

d. Telephone answering devices to automatically disseminate or receive information in a "hands off" mode (i.e., automated attendants, interactive voice response).

Note: Additional policy and guidance is located on the Commandant (CG-642) Telecommunication Systems Division portal site (Telephony Systems and Peripheral Equipment document): https://cgportal2.uscg.mil/units/cg642/SitePages/Home.aspx.

3. Telephone Management and Policy.

   a. Telephone Management Programs. The Telephone Management Program shall be administered by the C4IT SC. Local programs shall be implemented and administered by regional base C4IT division. Local programs shall ensure the following:

      (1) Personnel are aware of the proper and effective use of telephone services to include policies on personal use as detailed in section E.3.b of this Chapter;

      (2) CG DARS are familiar with and comply with applicable Federal Management Regulations and Federal Acquisition Regulations for procuring and managing telephone services. DARs shall semi-annually check all invoices or accounts under their ownership to certify the accuracy of the inventory and associated charges. The schedule for these checks is the end of the first and third quarter of each fiscal year. All unnecessary equipment and features shall be removed;

      (3) An acceptable standard grade of service is maintained, as defined:

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

         (b) The Networx contract provides seven calls in 100 (P07) blockage.

      (4) Where practical, consolidated or common user systems are used to provide service to multiple CG units; and

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

   b. Telephony Policy for Personal Use of Government Office Equipment. Current policies regarding authorized, inappropriate, and prohibited uses of CG office equipment are outlined in Reference (k). Commands are authorized to approve additional personal use on a case-by-case basis. The following section defines the policy for personal use of government telephone systems.

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

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

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

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

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

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

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

(2) Long Distance Calls. All other long distance calls not related to assigned duties that must be made during normal working hours shall be:

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

(b) Made to a toll-free number;

(c) Charged to a personal credit card; or

(d) Collect.

(3) Requirements For All Calls. The following policy pertains to all local and long distance calls:

(a) Shall not adversely affect an individual's or other's performance of official duties; and

(b) Shall be of reasonable duration and frequency.

c. Voice Systems Policy. The following policy applies for CG voice telephony systems:

(1) 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);

(2) DSN services are not authorized for CG Auxiliary members; and

(3) 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 C4IT

SC. Units requesting toll-free service are responsible for charges incurred by the service.

4. Cellular Telephones. Unconstrained use can result in excessive equipment procurement and on-air costs. Units shall closely monitor cellular telephone use. Additionally, units shall establish local policies and procedures for effective management and oversight of locally acquired cellular equipment and services. The following section provides additional policy for cellular telephones.

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

   b. Units shall be responsible for cellular phone management, life-cycle costs and usage fees.

   Note: Cellular systems do not provide COMSEC unless a global security module (GSM-SM) for mobile communication security is used.

5. Federal Calling Cards. TISCOM shall act as the enterprise federal calling card manager 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 DAR ordering guidelines. Unit calling card administrators shall locally manage calling card inventory for their unit, notifying TISCOM of changes in card requirements (e.g., personnel transfers), requests for new cards, and inventory validation. GETS cards are not federal calling cards and therefore do not fall into this policy. The following section outlines specific federal calling card policy for CG personnel.

   a. Federal calling cards shall not be issued for non-government business.

   b. Use of prepaid calling cards with commercial airline air phones and commercial railway phones is strictly prohibited.

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

   d. CG Reservists are authorized to use federal calling cards for official use while preparing or arranging for active duty and while in an active duty status.

   e. CG Auxiliary personnel are not authorized federal calling cards.

6. Local Telephone Directory Listing. To minimize delay in reporting distress cases, adequate directory listings with correct telephone numbers shall be arranged with local telephone companies. Units shall ensure their local telephone company's directory list

managers provide the necessary information necessary to keep the listings current. In addition,

a. Directories should include area, district, and sector command centers in the AOR; and

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

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

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

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

b. District commanders, after evaluation of local programs, must determine their own levels of participation.

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

9. Caller Identification (ID). Caller ID services shall be utilized 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 (ANI) services as standard features.

F. Satellite Communications. The CG utilizes commercial and military satellite communication for daily operations. The following section outlines the policy for commercial and military satellite communication services.

1. Commercial Satellite Communication (COMSATCOM). COMSATCOM includes Mobile Satellite Service (MSS), Enhanced Mobile Satellite Service (EMSS), and Fixed Satellite Service (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.

a. General. Commandant (CG-642) is the asset manager for CG COMSATCOM requirements approved by Commandant (CG-761). Commandant (CG-642) coordinates with the C4IT SC as necessary to meet approved COMSATCOM requirements.

b. 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) EMSS designates the "enhanced" form of Iridium mobile satellite communications and includes a secure capability, the ability to direct dial from a Public Switched Telephone Network phone to the 808 area code, and the ability to communicate with the DSN.

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

c. Use of Commercial Satellite Communication (COMSATCOM). 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 C4IT SC and TISCOM.

d. General Policy for Satellite Phones. Requirements for satellite phones vary throughout the CG. However, airtime costs can be excessive with unconstrained use. Satellite telephone use shall be closely monitored by the command to minimize cost. The following satellite phone policy applies:

(1) Satellite phones shall not be used when terrestrial phone service is available;

(2) Area and district commanders can approve the use of satellite phone equipment to augment CGTS operationally; and

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

e. Iridium Satellite Phones. 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. Further information pertaining to EMSS Iridium satellite phones is as follows:

(1) Iridium satellite phones provide no communication security unless the secure module is used with an activated DOD subscriber identity module (SIM) on a securable, tamper-sealed handset.

(2) Iridium satellite phones are portable electronic devices subject to policies and procedures outlined in Reference (j). Further safeguarding guidance is as follows:

(a) EMSS Iridium satellite phones become classified when connected to the Iridium security module (ISM) and the user personal identity number (PIN) has been entered allowing secure communications;

(b) The ISM is a cryptographically controlled item (CCI) and shall be stored and shipped according to Reference (g);

(c) The user PIN shall be stored in a safe place and is unclassified (FOUO) when not stored with the associate ISM; and

(d) Loss of the ISM with or without the phone is a reportable physical incident requiring report per Reference (g).

(3) Further policy regarding Iridium satellite phones is as follows:

(a) CG Iridium phones obtain airtime services in one of two ways; either through DISA or a commercial provider. Reference (a) contains procedures for identifying airtime service type for Iridium satellite phones. Commands shall identify which airtime service the unit Iridium satellite phone uses to prevent the misuse of Iridium equipment;

(b) Use of DISA Iridium satellite phones (non-commercial) for morale calls is authorized per Reference (k), at the commanding officer's discretion. DISN MSS is procured through DISA and consists of a monthly flat rate per phone with unlimited use;

(c) Iridium phones on commercial service plans are designated for contingency operations. These Iridium phones can 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;

(d) Unless permanent shipboard mounts are installed per an approved Time Compliance Technical Order (TCTO), Iridium satellite phones are to be used with the handset only. Temporary magnetic mount of external antennas is authorized and can be used as deemed necessary by the command; and

(e) Communication checks on Iridium satellite phones used less than twice a month shall be conducted monthly to ensure the equipment is ready for operations. Phones capable of secure communication shall be tested in both clear and encrypted modes.

(f) Commands shall be responsible for maintaining a unit inventory containing the Iridium phone number, Iridium phone model number, SIM number, and the International Mobile Equipment Identity (IMEI) number.

(g) Units shall contact the LANTAREA, PACAREA, or TISCOM (TIS-311) Iridium phone manager for further guidance on tamper seals and/or ISMs.

2. Military Satellite Communication (MILSATCOM). MILSATCOM is the DOD satellite constellation providing near global operational communications for military aircraft, ships, and ground stations to meet the requirements for rapid, reliable, and secure communications throughout DOD. The CG requires access to MILSATCOM for interoperability with the USN and DOD in time of war (U.S.C. 14 § 3), to meet CG, DHS, and interagency missions in peacetime and for communicating with U.S. allies and other government agencies. USN support to meet MILSATCOM interoperability requirements is outlined in Reference (d). The CG uses both the extremely high frequency (EHF) and UHF frequency bands for MILSATCOM.

a. Definition.

(1) Demand Assigned Multiple Access (DAMA). DAMA multiplexes several baseband systems or users onto one 25 kilohertz (kHz) channel to increase the number of available channels. One 5 kHz DAMA channel can support one 2.4 kilobits-per-second (kbps) voice time slot and one point-to-point connection. One 25 kHz DAMA channel can support up to five 2.4 kbps voice or data circuits.

(2) Integrated Waveform (IW). IW is a recently implemented UHF satellite communication (SATCOM) waveform which requires software and/or hardware upgrades to existing UHF SATCOM terminals. Using legacy DAMA, this waveform increases the UHF SATCOM channel availability allowing SATCOM planners the ability to mitigate any potential Mobile User Objective System (MUOS) schedule delays or UHF SATCOM constellation failures.

(3) Interim Polar System. The Interim Polar System provides users only low data-rate EHF access and does not have the ability to cross-link to the UHF Follow-on (UFO) constellation. There is limited infrastructure in place for Interim Polar System communications support.

(4) Joint Tactical Radio System (JTRS). JTRS is a new generation multi-band radio system, developed by the DOD, to replace existing MILSATCOM terminals. JTRS radios are compatible with the MUOS satellites and provide a variety of waveforms, including MUOS, to access the on-demand 2.4 to 64 kbps channels for voice and data services.

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

(6) Mobile User Objective System (MUOS). MUOS is replacing the end-of-life UFO system. MUOS is capable of serving additional users with greater mobility, capacity, and quality of service. MUOS is a limited protected narrowband (64 kbps and below) satellite communication system that supports a worldwide, multi-service population of mobile and fixed-site terminal users. The MUOS legacy payload can provide interoperability with the legacy terminals until the MUOS constellation reaches full operational capability.

(7) Multi-band Radio. Radios that can operate in more than one band.

(8) 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)).

b. MILSATCOM Capabilities. MILSATCOM capabilities are in the following:

(1) For a complete overview of approved MILSATCOM systems, equipment, and ancillary equipment, refer to C3CEN portal page: https://cgportal2.uscg.mil/units/c3cen/SitePages/MILSATCOM.aspx; and

(2) For a complete overview of EHF systems, processes, point of contact, and procedures, refer to the following site: https://cgportal2.uscg.mil/units/tiscom/SitePages/Supported%20Systems.aspx.

c. Military Satellite Communication (MILSATCOM) Use. CG specific MILSATCOM circuits are listed in Chapter 7 of this Manual. The following are examples of additional DOD circuits authorized for CG use:

(1) Satellite high command (SATHICOM) (USN tactical voice);

(2) Joint Interagency Task Force (JIATF) air (JIATF South tactical voice);

(3) JIATF surface (JIATF South tactical voice);

(4) Common User Digital Information Exchange Subsystem (CUDIXS). CUDIXS is used for tactical record messages with a Top Secret or below classification level;

(5) Fleet Satellite Broadcast Subsystem. The Fleet Satellite Broadcast Subsystem is the USN record message system authorized up to the top secret classification level but currently used for the classification level secret; and

(6) Columbian Navy (COLNAV). COLNAV is the JIATF Columbian Navy circuit.

d. Roles and Responsibilities: 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. United States Northern Command (NORTHCOM) is the DOD MILSATCOM sponsor for the CG. NORTHCOM validates all CG missions requiring access to DOD Satellite channels in the military UHF/EHF spectrum. The following section outlines CG specific roles and responsibilities for MILSATCOM capabilities.

(1) Coast Guard (CG) Shore and Afloat Assets.

(a) Commandant (CG-761) is the sponsor for all enterprise CG MILSATCOM requirements for CG shore and afloat assets.

(b) Commandant (CG-64) is the program manager for all shore/afloat MILSATCOM radio procurements and provides the technical standards for all Commandant (CG-9) C4IT future shore/afloat MILSATCOM system acquisitions Commandant (CG-64) directs the C4IT SC to provide solutions to meet validated MILSATCOM requirements.

(c) C3CEN is the system development agent and system support agent for all MILSATCOM equipment (less aviation assets) throughout the CG.

(d) The area C4IT division manages MILSATCOM operations, status, and capability requests for shore and afloat assets.

(e) TISCOM is the system development agent and system support agent for all EHF equipment support, access procedures, and training.

(2) Coast Guard (CG) Aviation Assets.

(a) Commandant (CG-711) is the sponsor for all aviation MILSATCOM requirements.

(b) Commandant (CG-41) is the integration manager for all CG aviation platforms.

(c) The Aviation Logistics Center (ALC) leads all aviation MILSATCOM platform integration. The ALC will collaborate with C3CEN to ensure enterprise MILSATCOM configuration management is consistent for aviation assets.

(d) The area C4IT division manages MILSATCOM operations, status, and capability requests for aviation assets.

e. Department of Defense (DOD) Satellite Database. Commandant (CG-64) manages the CG MILSATCOM mission data entries in the DOD satellite database. This includes annual review/update, removal, and submission of new entries through NORTHCOM for review by the Joint SATCOM Panel.

f. General Military Satellite Communication (MILSATCOM) Policy. MILSATCOM policy is outlined in the following paragraphs.

(1) System Configuration. All MILSATCOM system configuration changes at shore or afloat units shall be conducted per Reference (i). For guidance on MILSATCOM system configuration changes for aviation assets, contact COMDT (CG-41).

(2) Terminal Base Address (TBA). The TBA is a unique address assigned to identify each MILSATCOM system. All MILSATCOM terminals shall have a TBA for access to a MILSATCOM DAMA channel. Units that obtain any new or previously owned MILSATCOM systems shall submit a TBA request to C3CEN.

(3) Satellite Access Requests. The submission of a satellite access request to NORTHCOM for all MILSATCOM system access is required per Reference (l). All satellite access requests shall be submitted via the Joint Integrated Satellite Communications Tool (JIST). Area C4IT divisions shall submit quarterly MILSATCOM satellite access requests to NORTHCOM.

(4) Extremely High Frequency (EHF) Access. Units shall submit a satellite access request to NORTHCOM no less than 30 days prior to the start of the mission for all EHF access per Reference (l). For specific guidance, cutters shall use the EHF Satellite Access Request Standard Operating Procedure provided by the system support agent. Cutter operators are authorized to contact NORTHCOM after request submission to verify the request was properly submitted. The area C4IT division is responsible to facilitate EHF related communication issues between the cutters and servicing EHF facility.

G. Other Telecommunication Services. The following section outlines policy for other telecommunication services.

1. Pagers. The area or district commander can operationally approve paging equipment for CG personnel.

2. Facsimile (FAX). FAX is 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 DHS Management Directive MD Number 11042, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, "Unless otherwise restricted by the originator, FOUO [For Official Use Only] information may be sent via non-secure FAX. However, the use of a secure 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. The holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator." If specific guidance on FAX is needed, individual commands shall check with their area C4IT or district telecommunications division/branch.

   a. Secure FAX. The term "secure facsimile" refers to a combination of the secure telephone equipment (STE) and a FAX machine which meets the standards outlined in Reference (m). Minimum security requirements for the handling and control of STE terminal equipment and associated cryptographic keying material (KEYMAT) can be found in Reference (g).

   b. Security. Each command shall 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 References (g) and (n).

3. Video Services on Coast Guard One Network (CGOne). Video services on CGOne shall be as follows:

   a. CGOne is not designed to support live streaming video for large number of users. Real-time video streaming requests shall be prearranged and authorized by Commandant (CG-64) via the area C4IT division (LANT-6/PAC-6).

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

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

d. The standard video resolution for CG-wide videos shall be 640 x 480 pixels. Videos requiring a higher resolution for CG-wide viewing shall be approved by TISCOM prior to publishing.

4. Nationwide Automatic Identification System (NAIS). The following Automatic Identification System (AIS) policy applies:

a. Only unclassified information shall be transmitted on AIS. CG commands equipped with AIS transmit capability are authorized to send FOUO/SBU information using an encrypted message; and

b. AIS safety related text messages are not designed or intended to serve as formal distress alerts. Therefore, AIS shall not be relied upon as the primary means for broadcasting distress or urgent communications, nor used in lieu of Digital Selective Calling (DSC) radios which are designed to process distress messaging.

c. AIS may be used to augment GMDSS and provide the added benefit of being seen on radar or chart displays, in addition to being heard (via text messaging) by other AIS users within VHF radio range. For further guidance, see USCG Safety Alert 5-10 located at the following website: http://www.navcen/uscg.gov/pdf/AIS/0510.pdf or refer to International Maritime Organization's (COMSAR) Circular 46, Use of AIS Safety-Related Messaging in Distress Situations.

CHAPTER 4 COAST GUARD (CG) TELECOMMUNICATION REQUIREMENTS, PLANS, AND ACQUISITION

A. General. Telecommunication requirements, plans, and acquisition management 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 Requirements. Established CG telecommunications requirements can be found in the following:

1. Operational Communication Requirements Management. The Assistant Commandant for Capability (CG-7) oversees the CG's requirements management process as outlined in Requirements Generation and Management Process, Pub 7-7. Commandant (CG-761) publishes documents outlining CG command, control, communication, and computers (C4) that include telecommunication requirements; and

2. Radio Frequency Requirements. Per Chapter 3 and Reference (h), requests for frequency assignments and modifications to assigned radio frequencies or other spectrum dependent equipment, whether for fixed or mobile use, shall be endorsed by the district telecommunications division/branch and sent to the regional base C4IT division for coordination with area commanders and national level approval.

C. Telecommunication Planning. The following section outlines the policy and guidelines for developing telecommunication plans.

1. Communications Guard. The Glossary of Communications-Electronic Terms, ACP 167 (series), defines guard (radio communication) as "to maintain a continuous receiver watch with transmitter ready for immediate use." Based on this definition, the following policy for maintaining communication guards when developing telecommunication plans applies:

   a. Continuous Guard. 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; and

   b. Uninterrupted Guard. During an uninterrupted guard, the operator can switch to another frequency to make a transmission, but shall maintain monitoring the frequency that requires the uninterrupted guard.

2. Telecommunication Plans. Areas, districts, and units shall prepare and issue telecommunications directives appropriately for the organizational levels as specified

below.

a. Area Telecommunication Plans. The area commander shall prepare and promulgate area telecommunication plans (Annex K to Area OPLAN). Annex K to Area OPLAN provide telecommunication policy, operating procedures, and general information. The following subject matter, as a minimum, shall be included in the Annex K to Area OPLAN:

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

(2) Cutter, aircraft, shore-side, and Auxiliary communication (include operations normal reporting requirements);

(3) Lost communication procedures for cutter, aircraft and shore-side;

(4) Broadcast notice to mariners (BNM) schedules (referred to as marine information broadcasts in previous editions of this Manual) and special broadcast instructions;

(5) List of units and call signs;

(6) COMSEC responsibilities;

(7) Landline circuit/network arrangements and/or configurations;

(8) Casualty reporting and restoration procedures;

(9) Procedures for requesting additional telecommunication resources and obtaining operational approval;

(10) Radio frequency planning and frequency authorization procedures and references (http://cgweb.rss.uscg.mil/communicationsportal);

(11) Emergency preparedness activities;

(12) Contingency and continuity of operations (COOP) procedures and activities;

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

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

b. 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 generally follow the format of Annex K to Area OPLAN and shall satisfy requirements found in Reference (o).

c. Unit Telecommunication Plans. Individual commands shall prepare locally-generated telecommunication plans, aligned with the area Annex K to Area OPLAN and district supplements. These plans identify administrative requirements, frequency plans, COOP, and operational procedures unique to the unit. Duplicate material found in other publications only in the interest of continuity or completeness.

3. Radio Frequency Plans. All units with mobile and portable VHF and UHF tactical radios shall develop and maintain radio frequency plans, which shall include details for use of all fixed and mobile radio frequencies used by the unit for routine and non-routine operations. The following section provides further guidance pertaining to radio frequency plans.

   a. Standard Frequency Plans. Commandant (CG-65) established CG-wide VHF and UHF standard radio frequency plans. All units shall include these standard plans in their VHF and UHF radio frequency plans and the supporting code plugs in their mobile and portable VHF and UHF radios.

   b. Code Plugs. A code plug is a program loaded into the radio that provides dedicated frequencies used to transmit and receive, radio frequency power output, carrier squelch/coded squelch, signaling modes, and other special features that need to be enabled.

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

      (2) Standard code plugs and radio frequency plans, along with the restrictions and guidance for use, and other CG tactical radio support resources are available on the Commandant (CG-652) tactical radio intranet site: http://cgweb.rss.uscg.mil/communicationsportal. This is the CG's authoritative source for code plugs and frequency plans.

      (3) C3CEN has sole responsibility to develop, manage, and support CG standard code plugs based on the CG-wide frequency plans established by Commandant (CG-652).

      (4) Units shall maintain the standard code plug in all VHF and UHF radios.

      (5) Changes to the standard code plug are published by the C4IT SC via record messages.

(6) CG standard code plugs and associated encryption assignments shall be appropriately handled as SBU material and shall remain internal to the CG unless specifically authorized for release by the area C4IT divisions (LANT-6/PAC-6).

(7) CG districts can authorize adding local zones of convenience to the standard code plug. The district telecommunications division/branch shall closely manage local zones of convenience to limit interoperability complications and ensure proper frequency authorizations are obtained prior to loading and use. The C4IT SC (C3CEN) provides guidance but is not responsible for providing support for local zones of convenience. Support to CG units for developing, modifying, and loading local code plugs, to include district zones of convenience, shall be provided by the local units supporting base C4IT division/ESD.

(8) CG command and control channels are selectable for either encrypted or clear operation. This 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.

(9) The district telecommunications division/branch can authorize units in their AOR to enable the 'channel' knob on their portable tactical radios.

(10) The base C4IT division/ESDs shall provide code plug support to aviation units and for aircraft radios. The following section provides policy for the standard aviation RT-5000 VHF/UHF code plug.

(a) 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.

(b) The C4IT SC develops, maintains, and provides tier-3 support for the CG standardized code plug and RPWIN files for all RT-5000 tactical radios. The standard code plug is developed per telecommunications 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 C4IT SC.

(c) In addition to the baseline code plug, air stations (AIRSTA) shall include local frequency requirements in their code plug. The AIRSTAs regional base C4IT division/ESD develops, maintains, and provides customized RT-5000 baseline code plugs and RPWIN file programming support to meet the AIRSTAs local frequency requirements.

(d) AIRSTAs shall submit requests for local frequency requirements to the district telecommunications division/branch via the spectrum manager assigned to the district. The district telecommunications division/branch shall forward the approved local frequency plan to the regional base C4IT division for modification to the AIRSTA code plug. Code plugs and RPWIN files are available for download at:

http://cgweb.rss.uscg.mil/communicationsportal/default.aspx;

(e) CG districts may 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; and

(f) The Custom and Border Protection (CBP) National Law Enforcement Communications Center (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.

4. Contingency Communications Plans (CCP). Operational commanders shall develop and maintain a CCP for communications equipped units under their AOR. This policy is established to ensure expeditious restoration of communications, in a contingency situation, to support local operations and to protect the safety of life and property. A Contingency Communications Plan (CCP) Guide is located in Reference (a) for further guidance on CCP development. Each CG district and sector is unique and shall have a tailored CCP for the units AOR, to include a plan for establishing and maintaining interoperable communications with local partners.

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

6. Incident Management Communications. The U.S. Coast Guard Incident Management Handbook (IMH), COMDTPUB P3120.17 (series) provides communication responsibilities and policy for CG personnel during response operations.

7. Marine Bands. Units not capable of digital communications and units communicating with platforms without digital communications capabilities are authorized use of the following maritime channels in analog clear or 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:

   a. VHF-FM Channel 16 (156.800 MHz) - International calling and distress frequency;

   b. VHF-FM Channel 21A (157.050 MHz) - Maritime/air/ground SAR working frequency;

   c. VHF-FM Channel 23A (157.150 MHz) - Maritime/air/ground SAR working frequency;

   d. VHF-FM Channel 81A (157.075 MHz) – Interagency response channel for pollution response operations. Use only when no other listed channel is available; and

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

8. Recording or Monitoring Equipment. The following policy applies to the use of recording or monitoring equipment:

   a. Secretary Department of Homeland Security (SECDHS) Policy. Per Personal Use of Government Equipment, Department of Homeland Security Management Directive System MD Number 4600.1, telephone calls may be monitored or recorded for legitimate business purposes such as providing training, instruction or protection against abusive calls. Personal phone conversations and business telephone calls will not be routinely monitored. Exception: Due to the CG's SAR mission, the use of telephone recording equipment is authorized as indicated in section C.8 of this Chapter;

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

   c. Recording of Voice Communication Circuits. Digital voice logger (DVL) and R21 recording equipment is required at all CG units (less stations, aircraft, and vessels under 87 feet in length) to record all telephone and voice radio communications where such communications relates to the safety of life and property, including but

not limited to air safety, maritime safety, SAR, and CG tactical communication operations. If the recording contains protected or secure communications, the recording shall be safeguarded per Reference (j) or (n). The CG does not require beep tones or prior consent for the recording of these conversations; and

d. Other Authorizations. Authorization to install and use monitoring equipment for situations not listed in this section must be obtained from the units servicing legal office.

9. Interoperability. Use of the CG's short range communication infrastructure, R21, for interoperability is strongly encouraged. When using R21 mixed-mode patch circuits, the following policy applies:

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

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

   Note: Available interoperability frequencies can be found at: http://cgweb.rss.uscg.mil/communicationsportal.

10. MINIMIZE. MINIMIZE is a term, not acronym, used by command authorities to clear military telecommunication circuits of all nonessential traffic in an actual, simulated, or anticipated emergency. This includes, but is not limited to, record messaging systems, email (to include attachment size limitations), CGOne, SIPRNET, JWICS, telephone and cellular circuits, chat, internet, social media, and video teleconferencing use.

    a. Authorization. Authorization to implement MINIMIZE shall be as follows:

       (1) Normally, the unified commands issue the MINIMIZE order;

       (2) Designated commanders can request other commanders or friendly foreign countries to impose MINIMIZE;

       (3) Commanders can request the Chairman, Joint Chiefs of Staff (CJCS) impose MINIMIZE on users in other areas that originate traffic destined for addresses in the area under MINIMIZE;

       (4) The commanders or chiefs of other agencies can be requested to impose MINIMIZE on all users required to communicate with activities in the MINIMIZE area, or whose telecommunication services passes through the telecommunication facilities of the area under MINIMIZE; and

       (5) All commanders and unit commanding officers can impose MINIMIZE within

their AOR unless specifically denied by higher authority. When MINIMIZE is imposed upon worldwide networks, area and district commanders can authorize relaxed conditions of MINIMIZE over networks or circuits entirely within their control.

b. Implementation. Implementation of MINIMIZE shall be as follows:

(1) The CJCS or a commander of a unified or specified command will impose MINIMIZE upon all or part of their areas of command responsibility by general record message. These general record messages shall automatically apply to CG forces in the area specified;

(2) CG record messages implementing MINIMIZE shall include the applicable operational commander, area commander, district commander, and Commandant as addressees. Unless otherwise stated in the record message, the MINIMIZE is effective for all communication circuits; and

(3) Procedures to request CG-wide MINIMIZE are in Reference (a).

c. Enforcement. Enforcing MINIMIZE is a command responsibility, and is imposed upon users, not information systems and telecommunication networks.

d. Exemptions. 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 reports (CASREP);

(7) Aircraft and fleet unit movements;

(8) Continuing research and development programs vital to national interest; and

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

e. Record Messages. Commands shall specifically designate a limited number of users

with record message release privileges during periods of MINIMIZE. The commanding officer shall not permit release of non-urgent record messages when MINIMIZE is imposed on the record messaging system. Per Reference (p), CG record messages that meet the criteria to be released during MINIMIZE shall include the following as the last line of the text: "Released by (name and rank/grade)."

11. Additional Telecommunication Planning Information. When making telecommunication plans, the following additional items shall be considered:

    a. Communications capabilities of CG and/or other assets assigned;

    b. COMSEC requirements;

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

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

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

D. Telecommunication Services and Equipment Acquisition. Acquisition and use of telecommunication services and equipment by federal agencies is subject to significant legal and regulatory restrictions. The following sections outline the policy for procuring telecommunication services and equipment.

1. New Telecommunication Service Requests (Excluding Enterprise Data Network and Telephony Services). All new requests are subject to requirements validation by Commandant (CG-761) and final approval by Commandant (CG-64). Units shall follow the Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Capabilities, and Requirements Oversight Panel (CROP) process for all new telecommunication service requests, except requests for network and telephony services, per Reference (a) (See section D.3. of this Chapter for network and telephony service requests). Systems installed outside the C4ISR CROP process are subject to removal. Refer to the following documents prior to initiating new requests:

    a. Requirements Generation and Management Process, Pub 7-7;

    b. C4ISR Operational Requirements Document; and

    c. Long Range and short range telecommunication requirements document (under development by Commandant (CG-761)).

2. Radio Systems Procurements.

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

      (1) The C4IT SC is the only authorized procurement authority for microwave point-to-point wireless services; and

      (2) Once new microwave service has been validated and approved, microwave wireless transmission services shall be funded by the local unit and their regional telecommunication managers.

   b. VHF/UHF Land Mobile Radio Procurements. Units determining a need for VHF/UHF radio assets shall adhere to the following policies:

      (1) The C4IT SC is the only authorized procurement authority for land mobile radio procurements; and

      (2) The procurement and use of non-licensed or non-intrinsically safe two-way radios, such as Family Radio Services and General Mobile Radio Service is not authorized for CG operational applications. Requests for approval or waiver will be denied.

      Note: See Reference (a) for VHF/UHF land mobile radio procurement procedures.

   c. 800 Megahertz (MHz) Radios. The procurement of 800 MHz radios is not authorized unless the CG unit is requested and authorized in writing by a state or local government agency for interoperability. See Chapter 3 of this Manual for further information regarding authorization policy. The procurement and support of 800 MHz radios needed to meet these unique local or regional interoperability requirements shall be a unit expense.

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

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

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

      (2) Designated Agency Representatives (DAR). DARs are field representatives

assigned to the regional base C4IT division and other designated commands authorized and trained to "order" telecommunication services. The following applies:

(a) CG DARs are the only authorized agents allowed to place orders for telecommunication circuits and services (excluding cellular wireless, but including microwave point-to-point wireless services and Internet) from approved sources and shall use the most current policy and practices promulgated by the C4IT SC;

(b) DAR authority is restricted, limited, and managed by the DAR administrator at TISCOM; and

(c) DARs shall be designated in writing by the agency DAR administrator and certified as contracting officer's representatives (COR).

b. Enterprise Data Network Service Requests. Area and district commanders, unit commanding officers, and directorates/special staff divisions at CG headquarters shall submit requests for enterprise data network services to TISCOM via their chain-of-command via CG memorandum. See Reference (a) for a list of information that is required to be included in the request.

c. DISN/DOD/Other Network Requests/Modifications. Requests or modifications for DISN, DOD, or other department or agency network services shall be submitted via official CG memorandum via district telecommunications division/branch or area C4IT division to the C4IT SC as "requests for service".

d. Telephony Requests/Modifications. Requests or modifications for DISN, DOD, or other department or agency telephone services shall be submitted via official CG memorandum via district telecommunications division/branch or area C4IT division to the C4IT SC as "requests for service".

e. Voice DCS Services. Requests for voice DCS services (e.g., DSN) provided by DISA, joint staff, DOD, or other department or agency service, or for service changes, shall be submitted in writing via area C4IT division (LANT-6/PAC-6) with supporting rationale to TISCOM thru the C4IT SC.

f. Cellular Equipment/Services. Unit commanding officers, officers-in-charge and office chiefs are permitted to procure cellular equipment and usage services from any vendor; however, when CG email will be used in conjunction with the device, units much purchase specific devices from an approved vendor. The approved vendor list is located on the TISCOM CG Portal site. For further instructions concerning cellular devices, members shall refer to Reference (j).

g. Pagers. The following policy applies:

(1) Pager service shall be leased; and

(2) Units shall be responsible for the equipment and service costs.

h. Non-Appropriated Funds Activity (NAFA). Government funded local exchange carrier (LEC) telephone or federal contract service can be provided to NAFA facilities. The use of these services is restricted to NAFA officers for the 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. The following section outlines additional NAFA policy.

(1) Pay telephone service shall be contracted between:

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

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

(2) Government funded local telephone or Networx services are not authorized for CG Credit Unions.

(3) Local telephone or Networx services paid with appropriated funds are not authorized for installation in residences. Government owned/leased representational facilities are exempt from this restriction. Appropriated funds can 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 for national defense purposes. This exception is for the installation of a STE in support of the Maritime Defense Zone mission and national security. Commandant (CG-6) must approve this service with concurrence from DHS.

i. Federal Telephone Services (FTS) Contracts. FTS contracts provide the CG with enterprise and local unclassified telecommunication services to include, but not be limited to, long distance switched and dedicated voice service, WAN (e.g., CGOne, SONET, ethernet), R21, audio/video conference calling, federal calling cards, internet gateways, toll free service, Large Capacity Disaster Recovery Network, fixed satellite services, enterprise product lines, and various other data and voice services to meet CG mission and unit requirements. The following section outlines policy for FTS services.

(1) Units requiring FTS services shall coordinate requests with the servicing DAR.

(2) Enterprise services are circuits and services that have been predetermined by Commandant (CG-65) to be supported by enterprise funding (e.g., CG central account) and include but are not limited to, CGOne, R21, NDRS, CSN, switched long distance service, federal calling cards, and long distance dedicated PBX trunks. Units requesting additions, moves and/or changes to enterprise services must route a service request, in writing, to TISCOM via their local servicing DAR and supply associated funding to support the new requirement(s).

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

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

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

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

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

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

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

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

4. Satellite Communications Acquisitions. Specific policy for satellite communication capability procurements is in the following section.

a. Iridium Satellite Phones. TISCOM is the sole provisioning agent for EMSS Iridium satellite phones on the DOD contract, including obtaining secure capabilities. In addition:

(1) The procurement of services from this contract must be approved by area or district commanders and Commandant (CG-64);

(2) DOD contract services can be procured using unit funds, but units shall order services through the TISCOM; and

(3) Units shall follow specific area procedures provided in the following link for repair or acquisition of new or replacement equipment: https://cgportal2.uscg.mil/units/tiscom/SupportedSystems/SitePages/Home.aspx.

b. MILSATCOM Equipment. The following policy applies for MILSATCOM equipment procurements:

(1) All new MILSATCOM radio procurements shall be completed following the C4ISR CROP process outlined in Reference (a).

(2) All new MILSATCOM radio procurements shall be coordinated with the unit EKMS manager to ensure proper tracking, transfer and storage;

(3) The unit EKMS manager shall advise the C4IT SC (BOD-IAB), via the EKMS immediate-superior-in-command (ISIC), of all new MILSATCOM radios obtained at the unit; and

(4) Requests specific to MILSATCOM ancillary equipment shall be directed to the C3CEN MILSATCOM system support agent for guidance prior to any purchase.

CHAPTER 5 COMMUNICATION SECURITY (COMSEC), COMMUNICATION SECURITY (COMSEC) MONITORING, ENCRYPTION, ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS), AND COMMUNICATION SECURITY (COMSEC) MANAGEMENT WORKSTATION IMPLEMENTATION

A. General. The protection of government telecommunications not intended for the general public is crucial to effectively planning and executing CG missions. Commands engaged in classified or sensitive operations shall exercise 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. This Chapter provides policy for COMSEC, encryption, EKMS, and the COMSEC management workstation implementation.

B. Communication Security (COMSEC). 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 INFOSEC, transmission security, emission security and physical security of COMSEC material"). 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. Definitions.

a. 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 Reference (f).

b. COMSEC Material Control System (CMCS). Logistics and accounting system used to distribute, control, and safeguard COMSEC material marked "CRYPTO". CMCS includes the COMSEC Central Offices of Record, crypto logistic depots, and COMSEC accounts. COMSEC material other than cryptographic keying material (KEYMAT) can be handled through the CMCS (See EKMS definition).

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

d. Electronic Key Management System (EKMS). An interoperable collection of systems developed by services and agencies of the United States government; a component of the CMCS. EKMS automates plans, orders, generation, distribution,

storage, filing, use, and the destruction of electronic key. It also assists with the management of other types of COMSEC material.

e. Emission Control (EMCON). EMCON is the procedure used to provide transmission security (TRANSEC) through control of all electromagnetic and acoustic radiations, including communication, radar, electronic warfare, and sonar. In addition, EMCON can be an effective tool for implementing low probability of intercept (LPI), low probability of detection (LPD), and low probability of identification (LPID). The following policy applies:

(1) EMCON can be imposed for non-COMSEC purposes (e.g., ammunition handling, fueling and radiation hazard evolutions such as man-aloft); and

(2) During EMCON imposition, no electronic emitting device within designated bands, including personal communication devices, shall be operated unless absolutely essential to the mission.

Note: Refer to Naval Communications, NTP 4 for more information on EMCON.

f. Emission Security (EMSEC). Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emanations from crypto-equipment or an information system. (See TEMPEST definition).

g. Encryption. The process of changing plaintext into ciphertext for the purpose of security or privacy.

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

i. 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.

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

k. Operations Security (OPSEC). OPSEC is an analytical process used to deny an adversary information- generally unclassified – concerning CG intentions and capabilities by identifying, controlling, and protecting indicators associated with CG planning processes or operations.

l. Protected Communication. Communications using unclassified or "Type III" encryption including data encryption standard (DES) or advanced encryption standard (AES) encryption.

m. Secure Communication. Communication using classified or "Type I" encryption to support classified information exchange.

n. Tactical Communications. Near-real time or real time communication supporting an ongoing CG operation.

o. Transmission Security (TRANSEC). Security controls applied to transmissions to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals. TRANSEC is that field of COMSEC which deals with the security of communication transmissions, rather than that of the information being communicated (see EMCON definition).

p. TEMPEST. A term, not acronym, referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

2. Classified Information Management Program. Measures designed to prevent unauthorized access to non-COMSEC classified equipment, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft. Deputy Commandant for Mission Support (DCMS-34) oversees the CG's classified information management program. For more information see Reference (n).

a. 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 in Reference (q).

b. Physical Security. Physical security is achieved within CG telecommunication facilities through guidelines promulgated in References (g) and (r).

c. Other Classified Material Control (CMC) Systems. The physical handling and storage of certain classified material falls under a CMC system per Reference (n), to include the following material:

(1) SCI;

(2) All Top Secret information;

(3) COMTAC information; and

(4) Classified NATO material.

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

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

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

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

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

   e. Commandant (CG-65). Commandant (CG-65) has overall COMSEC responsibility for the CG. Commandant (CG-65) 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.

   f. Command, Control, Communications, Computers, and Information Technology Service Center (C4IT SC). C4IT SC (BOD-IAB) serves as the principle agent, under direction of Commandant (CG-65), for COMSEC matters throughout the CG. C4IT SC (BOD-IAB) shall adhere to the following:

      (1) Commandant (CG-65) in coordination with C4IT SC (BOD-IAB), shall be responsible for updating and issuing COMSEC procedures throughout the CG;

      (2) The C4IT SC (BOD-IAB) promulgates detailed CG COMSEC procedures and exercises service-wide management and oversight of CG EKMS accounts; and

      (3) C4IT SC (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) KEYMAT Package.

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

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

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

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

(4) Review of COMSEC monitoring reports:

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

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

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

h. District Commanders. District commanders shall direct their units per area COMSEC instructions, and address their COMSEC and COMSEC monitoring needs to the cognizant area commander. In addition, district commanders shall:

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

(2) Provide oversight and management of the EKMS program within the AOR;

(3) Review COMSEC monitoring reports;

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

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

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

i. Commanding Officers. Commanding officers shall maintain 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:

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

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

(3) 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;

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

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

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

1. General. This section outlines certain responsibilities of area and district commanders and their legal officers in carrying out the requirements of Reference (s).

2. Definitions. Reference (s) contains a complete list of applicable definitions. However, the following definitions as applicable to COMSEC monitoring are provided:

a. Communication Security (COMSEC) monitoring. The act of listening to, copying, or recording transmissions of one's own official telecommunication to analyze the degree of security.

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

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 this Manual and References (a) and (s).

   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 Reference (k).

   b. With limited exception, no agency shall monitor CG telecommunication for COMSEC purposes without the express written approval of the Commandant (CG-00).

4. COMSEC Monitoring Notification. Notification of COMSEC monitoring existence can be accomplished by any of the following means, or combination thereof, if the legal officer considers the means chosen to be legally sufficient to achieve proper notification in terms of content, prominence, and specificity:

   a. Decals placed on the transmitting or receiving devices;

   b. A notice in the daily bulletin, plan of the day, or similar medium;

   c. A specific memorandum to users;

   d. A statement on the cover of official telephone book or communication directory; and

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

5. Legal Certification. The following policy for legal certification applies:

   a. Commandant (CG-65) shall ensure all the legal provisions of Reference (s) are met, reviewed and recertified every 2 years with applicable monitoring agencies;

   b. Users of government telecommunication systems shall be notified in advance that the use of these systems constitutes consent to monitoring for COMSEC purposes. The guidelines for providing this notification are in section C.4. of this Chapter;

c. Area legal offices 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 list of mandatory methods for COMSEC notification are in place at each unit within the AOR. When the annual legal review is completed, send report of compliance with Reference (s) via record message to Commandant (CG-65) no later than 15 AUG. See Reference (a) for the record message reporting procedures; and

d. Commandant (CG-65) shall ensure the CG is recertified so monitoring agencies may, if applicable, legally continue to provide COMSEC monitoring for the CG.

6. Unauthorized Disclosure. An unauthorized disclosure is any classified, SBU, PII item listed in the CG Critical Information List (CIL), Essential Elements of Friendly Information (EEFI) list or material that has been transmitted via an unauthorized method and results in a possible exposure of this information or material to unauthorized individuals. Unauthorized disclosure reporting procedures are in Reference (a).

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

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

a. Classified information shall be processed using NSA approved cryptography equipment and materials; and

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

2. Maritime Public Communication. Maritime public support communication shall not be encrypted.

3. Emergency Transmission Policy. When the commanding officer determines emergency action is mandatory to affect delivery, record messages of any classification can be transmitted via the lowest level cryptographically secured circuit. Additionally, under emergency conditions, information of any classification, except Top Secret, can be transmitted over any circuit using procedures in Allied Telecommunications Record System (ALTERS) Operating Procedures, ACP 128 (series) and Communication Instructions – General, ACP 121 (series). In such cases, the originating command shall:

a. Include the handling instruction "CLEAR TRANSEC OVERRIDE AUTH" after the classification; and

b. Report compromises or suspected compromises resulting from exercise of this authority per Reference (n).

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

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

   b. AES cryptographic 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; and

   c. COMSEC keying material from any source is not permitted in non-CG supported radios unless authorized by the C4IT SC (BOD-IAB).

5. Cryptographic Keying Material (KEYMAT) Effective Period. The effective date/time for the CG secure voice encryption keys (DES and AES) is the first working Monday of the month at 1130Z (federal holidays are not working days).

6. Encrypted Automatic Identification System (EAIS) Keyset. CG units are authorized to share unclassified Encrypted Automatic Identification System (EAIS) keyset with port partners and other government agencies in conjunction with joint port operations. Individual keysets are unclassified (FOUO), but shall not be passed through unencrypted means. The following section outlines the policy for EAIS keysets.

   a. On the last working day prior to the keyset change (federal holidays are not working days), CG units can distribute the keyset to agency technicians via protected communications, including AES encrypted tactical radio, encrypted voice phone (STE), or as a password-encrypted e-mail attachment. If using a password-encrypted e-mail attachment, a second email with a different subject line shall be sent containing the password to decrypt the attachment in the first email. Passwords shall conform to the following:

      (1) Be at least 8 characters in length;

(2) Contain a combination of alphabetic, numeric, and special characters;

(3) No repeats of the previous 8 passwords;

(4) Does not contain any dictionary word in any language;

(5) Does not contain any of the following: proper noun; the name of any person, pet, child, or fictional character; any employee serial number, social security number, birth date, phone number, or any information that could be readily guessed about the creator of the password;

(6) Does not contain any simple pattern, letters, or numbers (e.g., QWERTY, XYZ123);

(7) Does not contain any word, noun, or name spelled backwards or appended with a single digit or two digit "year" string (e.g., 98XYZ123); and

(8) Different from the user ID.

b. Single effective keysets can be written down for loading into the AIS transponder, but shall be destroyed once it is confirmed the transponder operates in the protected mode.

c. EAIS keysets are posted on the TISCOM SIPRNET website. SIPRNET equipped units can distribute the effective keyset to non-SIPRNET equipped subordinate commands using the STE in the secure mode.

d. The loss or possible compromise of keysets shall be reported immediately to the respective operational commander and C4IT SC (BOD-IAB) via the chain of command. Reports shall contain the keyset number(s) involved, detailed circumstances surrounding the loss, and an initial damage assessment.

Note: The keyset will be effective at 1800Z on the first working Monday of the month.

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

1. Units shall report immediately, via record message or email, the loss of a tactical radio or KVL to Commandant (CG-6421), C4IT SC (BOD-IAB), ADCON, OPCON, and tactical control (TACON).

2. ADCON shall notify CBP NLECC of the loss via a priority precedence record message (NLECC Orlando FL) or email (NLECC-WSOC@CBP.DHS.GOV).

3. If the lost tactical radio or KVL is loaded with encryption key, units shall check current EKMS requirements per Reference (g) for reporting the loss of cryptographic KEYMAT.

F. Electronic Key Management System (EKMS) Policy. The primary source for EKMS policy is Reference (g). CG specific EKMS policy is promulgated by numbered USCG COMSEC advisory messages. The advisory messages are effective until incorporated into Reference (g) and this Manual.

1. Electronic Key Management System (EKMS) Roles and Responsibilities. Reference (g) outlines EKMS management roles and responsibilities, selection and designation criteria, and the training requirements. To efficiently implement COMSEC responsibility:

   a. All CG personnel performing COMSEC related duties shall be thoroughly familiar with Reference (g);

   b. All CG personnel that install, operate, or maintain communication or cryptographic systems shall comply with current COMSEC or NIST publications and directives as applicable; and

   c. CG personnel shall immediately report any irregularities that impact COMSEC material as outlined in Reference (g).

2. Electronic Key Management System (EKMS) Program Management.

   a. Command, Control, Communications, Computers, and Information Technology Service Center (C4IT SC) (BOD-IAB). The C4IT SC (BOD-IAB) promulgates detailed CG COMSEC/EKMS procedures and exercises service-wide management and oversight of CG EKMS accounts. In addition, the C4IT SC (BOD-IAB) shall:

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

      (2) Coordinate internationally with coalition partners through NSA, State Department, other military services, and federal, state, local, and tribal law enforcement agencies to meet encrypted communication interoperability requirements for all CG missions;

      (3) In coordination with Commandant (CG-65), issue EKMS procedures and guidance throughout the CG;

(4) Serve as the COMSEC ISIC and service authority for all CG COMSEC (EKMS) accounts. However, account managers shall initially contact their area or district ISIC on COMSEC matters;

(5) Have primary responsibility for the CG EKMS Inspection Program; and

(6) Function 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.

b. Area Commanders. Area commanders shall assist in the management of the CG EKMS Program as follows:

(1) Designate in writing an EKMS ISIC to serve as an EKMS inspector and to assist CG commands in managing their EKMS accounts. EKMS ISIC responsibilities are outlined in Chapter 4 of Reference (g);

(2) Coordinate USN/CG EKMS support requirements with the appropriate USN fleet commander and promulgate area specific COMSEC instructions, requirements and procedures;

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

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

c. District Commanders. District commanders shall direct their units per area COMSEC instructions, and address their COMSEC needs to the cognizant area commander. In addition, district commanders:

(1) Shall 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;

(2) Shall initiate corrective actions as appropriate in response to COMSEC incidents; and

(3) Shall ensure compliance with the CEP per Reference (q).

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

(1) Be thoroughly familiar and comply with the specific responsibilities, duties, and required inspections as outlined in Reference (g).

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

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

e. EKMS Account Manager/Alternate Account Managers. EKMS account managers/alternates shall:

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

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

(3) Comply with specific responsibilities per Reference (g).

f. Local Element (LE) Personnel. LE personnel shall:

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

(2) Comply with specific responsibilities per Chapter 4, Article 465 of Reference (g).

3. Electronic Key Management System (EKMS) Inspections. EKMS accounts shall be inspected at least every 24 months. EKMS account inspections shall be conducted as follows, using References (g) and (t) for guidance. The following policy applies:

a. Area and district EKMS ISICs shall perform inspections of EKMS accounts under their cognizance; and

b. The C4IT SC (BOD-IAB) shall conduct an inspection of EKMS accounts held by headquarters units.

4. Electronic Key Management System (EKMS) Training Visits. All EKMS accounts shall receive a periodic NCMS Advice and Assist (AA) Training Visit within 90 days of the next scheduled formal inspection. The date of the most recent training visit shall be documented 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.

5. Communication Security (COMSEC) Material Control System (CMCS). The CMCS is the overall national system for the distribution, use and control of COMSEC equipment, cryptographic KEYMAT, and aids used to protect official government classified and SBU information. The CMCS provides for the physical security of COMSEC material. The CMCS is comprised of two major components:

   a. Electronic Key Management System (EKMS). EKMS includes cryptographic KEYMAT for all NSA encryption systems whose keys are loaded using standard fill devices.

   b. 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.

6. Maintenance of Cryptographic Equipment. The repair and replacement of all cryptographic equipment shall be coordinated through the C4IT SC (BOD-IAB). While specific procedures are detailed in Reference (g), commands are responsible for the proper maintenance and repair of cryptographic equipment, as follows:

   a. Repair of USN owned cryptographic equipment shall be accomplished per the EKMS-5 (series) Cryptographic Equipment Information/Guidance Manual; and

   b. Inoperative equipment shall be repaired or replaced by the servicing crypto repair facility (CRF) or other repair/maintenance facility.

G. Communication Security (COMSEC) Management Workstation (CMWS)Implementation Policy

1. Background. The CMCS and the account personnel that operate it have always been the back-bone of CG secure communication circuits and networks. This COMSEC account backbone has migrated from physical paper tape and manual tracking operation to a flexible, dynamic, and near real time automated electronic key distribution and management system. In addition to security, cost, and logistic considerations, this change was necessary to support the next generation of cryptographic communications equipment and systems being deployed. The following guidance applies:

   a. CG CMWS's with the Data Management Device – Power Station (DMD-PS) software installed shall be supported by CG managed regional COMSEC EKMS accounts. Use of these devices maintain compliance with national and USN COMSEC policy and procedures; and

b. This policy applies only to CG regional COMSEC EKMS accounts and subordinate CMWS DMD-PS Local Element (Issuing) (LE(I)). The operation of non-regional CG EKMS accounts remain unchanged. Although the CG operates as part of the USN COMSEC/EKMS program, only CG regional COMSEC EKMS accounts can interface directly with other EKMS accounts, the Common Tier-1, USN COMSEC Central Office of Record or national level COMSEC agencies. These policies definitively address new CG COMSEC operational doctrine and establish a robust CG COMSEC oversight program.

2. Definitions.

a. Regional Communication Security (COMSEC) Electronic Key Management System (EKMS) Account. A numbered COMSEC account utilizing the local management device/key processor (LMD/KP), Local COMSEC Management Software (LCMS), Common User Application Software (CUAS), Card Loader User Application Software (CLUAS), CMWS, Simple Key Loader (SKL), Really Simple Key Loader (RASKL) to interact with the Common TIER 1, USN, COMSEC Central Office of Record, and other EKMS accounts, to support multiple CMWS DMD-PS (LE(I))s, and/or other LEs and users.

b. Communication Security (COMSEC) Management Workstation Data Management Device – Power Station Local Element (Issuing) (CMWS DMD-PS LE(I)).

(1) A former EKMS LMD/KP account that has been converted to a CMWS DMD-PS LE that utilizes a CMWS running DMD-PS software in place of the LMD/KP to perform all normal COMSEC account functions. Interacts only with their assigned CG regional COMSEC EKMS account for all COMSEC material, electronic key, and COMSEC management functions. It may support other LEs and or LE(I) within their respective region with prior regional account concurrence; or

(2) An existing LE(I) that has been upgraded from an SKL to a CMWS DMD PS LE(I) to perform COMSEC management functions, key distribution, and can have a requirement to build specialized databases to load any of the numerous sophisticated next generation of end crypto equipment units (ECU) being fielded throughout the CG.

3. Coast Guard (CG) Communication Security Workstation (CMWS) Hierarchy. This policy does not address the EKMS Tier-0 (Central Facility), the Common Tier-1 Central Office of Record, or the USN Central Office of Record (as appropriate) since their operational roles and interaction with a CG regional COMSEC EKMS account are covered in national policy and Reference (g). This policy focuses on the CG COMSEC infrastructure and the regional COMSEC EKMS accounts relationship to the CMWS

DMD-PS LE(I)'s and their expanded role to standardize COMSEC operations throughout the CG. The CG operational CMWS hierarchy is described in the following section as shown in Exhibit 5-1.

a. Commandant (CG-65). The owner of all operational communications security functions within the CG.

b. Command, Control, Communications, Computers, and Information Technology Service Center (C4IT SC) (BOD-IAB). The C4IT SC (BOD-IAB) is the CG COMSEC Program Management Office and shall exercise overall authority for CG COMSEC operations, provide oversight of all CG EKMS accounts, including inter-service interoperability, compliance with national and USN policy, generate service specific policy, conduct inspections, and manage COMSEC equipment. In addition:

   (1) The C4IT SC (BOD-IAB) heads the process of converting an EKMS LMD/KP account to a CMWS DMD-PS LE(I) and shall coordinate with the respective CG area and the effected account;

   (2) The conversion of EKMS accounts to CMWS DMD-PS LE(I)s depends on the availability/capability of a regional EKMS account to assume another former EKMS accounts COMSEC support; and

   (3) Regional account availability is based on two main requirements:

      (a) The designated regional EKMS account has been installed (by the USN) with a fully functional EKMS Phase V suite of equipment capable of supporting CMWS DMD-PS LE(I) operations; and

      (b) The designated regional account has the manpower necessary (a minimum of 2 full time account personnel) to assume the additional duties and responsibilities of supporting multiple CMWS DMD-PS LE(I)s.

c. Area Immediate-Superior-In-Command (ISIC). The area ISIC shall provide COMSEC inspections, oversight, and training to all EKMS accounts. As the district EKMS/COMSEC accounts are converted to CMWS DMD-PS LE(I)s, the role of the district ISIC becomes that of the regional EKMS manager providing support and oversight to the increasing number of CMWS DMD-PS LE(I)s within their regional account AOR per this, national, USN, and CG policy and directives.

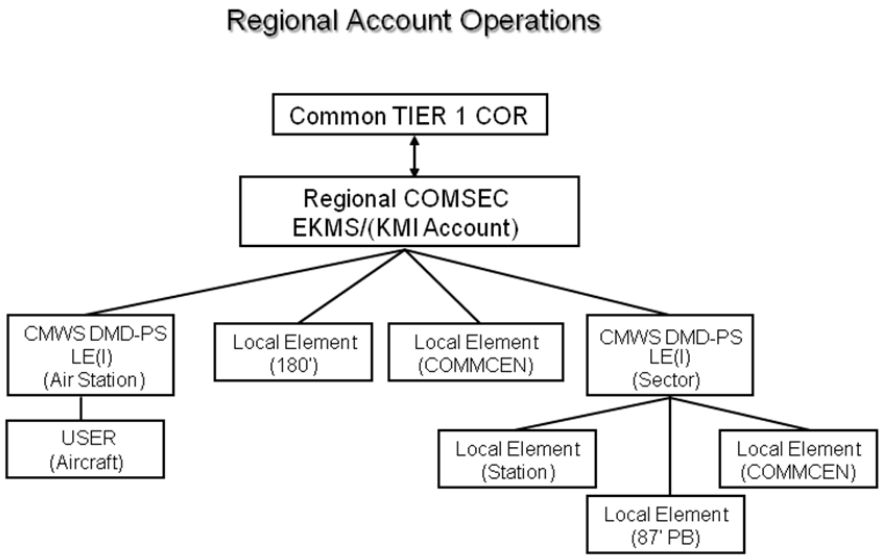
d. Regional Electronic Key Management System (EKMS) Accounts. Regional EKMS accounts shall utilize the LMD/KP and replacement follow-on equipment planned as part of the EKMS to KMI transition, to include the CMWS DMD-PS, SKL and RASKL. The regional EKMS manager is responsible to the area ISIC

and CG C4IT SC (BOD-IAB) for the management, training, and oversight of all CMWS DMD – PS LE(I)s and users within each region.

e. Communication Security (COMSEC) Management Workstation Data Management Device – Power Station Local Element (Issuing) (CMWS DMD-PS LE(I)). The end user directly subordinate to the CG regional EKMS account for the safe guarding and management of all COMSEC material issued to their unit and for providing training, oversight, and direction to their LEs and users.

f. Local Elements(LE)/Users. Operations and support is directly subordinate to either a regional EKMS account or a CMWS DMD – PS LE(I) that provides their COMSEC support.

Exhibit 5-1
CG Operational CMWS Hierarchy



4. Coast Guard (CG) Regional EKMS Account. Interacts with the Common Tier 1, the Central Office of Record, and CG COMSEC Management Office (C4IT SC (BOD-IAB)). The regional account manager provides COMSEC support and oversight to the CMWS DMD-PS LE(I)s and other users in their region The regional account and CMWS LE(I) shall operate within, but not limited to, the doctrine and responsibilities contained in this Manual.

5. Responsibilities. In regional EKMS account operations, all account personnel shall have duties and responsibilities for CMWS equivalent to their current EKMS roles as defined in Reference (g). The following section outlines additional responsibilities.

   a. Maintain a Letter of Agreement (LOA) between the regional account's commanding officer and all CMWS DMD-PS LE(I) commands.

   b. Provide all Tier-1/Central Office of Record functions (e.g., receipts, destructions, inventories) to include provisioning of all key and COMSEC material support to the CMWS DMD-PS LE(I)s assigned to their region.

   c. Provide database configuration control (including DMD-PS software and virus protection/Information Assurance Vulnerability Alert updates).

   d. Provide COMSEC oversight, including:

      (1) COMSEC incident reporting;

      (2) COMSEC practice dangerous to security reporting; and

      (3) Ensure COMSEC allowance meets mission requirements and is delivered in a timely manner.

   e. Develop and sustain a local training program for the CMWS DMD-PS LE(I) to maintain personnel proficiency/certification. This training shall be held in addition to the mandatory CMWS DMD-PS training required by Reference (g).

   f. Ensure quarterly spot checks are completed on all CMWS DMD-PS LE(I)s per Reference (g), (Note 1) of Art 465:

      "LE (Issuing) COs/OICs, including those in locations remote from the servicing or parent EKMS account, are responsible for conducting quarterly spot checks in accordance with Article 465 of this Manual. Servicing/parent EKMS accounts can require the reporting of spot check results; such a requirement should be spelled out in the LOA/MOU between the servicing command and the command being serviced, Note: Non CMWS DMD-PS LE and user spot checks are conducted IAW EKMS-1 (series)." The CMWS DMD-PS LE(I) shall report the results of quarterly spot checks to their respective regional account.

      Note: LOA/MOU examples are available on the CG Portal (C4IT SC EKMS).

   g. The regional account shall biennially conduct one on-site oversight and assessment for each CMWS DMD-PS LE(I) equipped unit within their region. The CMWS Oversight and Assessment Guide is available on the CG Portal (C4IT SC EKMS).

h. The regional account manager and COMSEC subject matter expert shall maintain professional relationships with program entities, Commandant, C4IT SC, area ISIC's, other service and national level agencies and be responsive to inquiries or requests from such as applicable.

i. The regional account shall ensure that all personnel whose duties require them to use COMSEC materials are properly cleared and that the privileges assigned formally authorize access to COMSEC material. This requirement shall be part of the LOA with the CMWS DMD-PS LE(I) who shall also require personnel who are issued COMSEC material to complete a COMSEC Responsibility Acknowledgement Form per Reference (g).

j. The regional account shall provide the CMWS DMD-PS LE(I) with written certification that the storage facility (i.e. safe and/or vault), through an oversight and assessment visit, is approved for storage of the highest classification of COMSEC material to be stored on a biennial basis.

6. Account Conversion.

a. Account closure procedures are contained in Reference (g). Converted accounts become LE(I) units. LE(I) units are subordinate to a regional account. In general, regional accounts include and oversee proper EKMS compliance for all LE(I) units under their operational chain of command and LE(I) units geographically in their AOR.

b. Upon final disestablishment of the account and commencement of full CMWS DMD-PS LE(I) operations, the regional account shall assume all COMSEC support, Central Office of Record functionality, and COMSEC oversight responsibility for the CMWS DMD-PS LE(I).

CHAPTER 6 COAST GUARD (CG) TELECOMMUNICATION ADMINISTRATION

A. General. This Chapter provides policy on daily communication logs, telecommunication records/reports retention and disposal, SAR distress and safety statistics, unit telecommunication inspections, and destruction devices. Additionally, this chapter covers false alert reporting policy and information pertaining to the Broadcast Quality Control Monitoring Program.

B. Telecommunications Service Priority (TSP) Services and Database. The TCO (TISCOM) shall maintain the DHS OEC TSP database for all telecommunication circuits. TSP is the regulatory, administrative, and operational system authorizing and providing for priority treatment (i.e., provisioning and restoration) of national security and emergency preparedness telecommunication services. TSP program management for the CG is delegated to Commandant (CG-6). Commandant (CG-6) further delegates ordering functions to the C4IT SC, the lead system support agent for telecommunication services. Management and ordering functions shall be per the most current policy and practices promulgated by the C4IT SC.

C. Telecommunication Reports. Procedures detailing telecommunication reports can be found in Reference (a). These procedures include submitting the following reports:

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

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

D. Telecommunication Records.

1. Intra/Inter-Area Dedicated Circuits. The C4IT SC and base C4IT division DARs shall maintain records of all intra/inter-area dedicated circuits. These records shall include, at a minimum, the following:

   a. Circuit number;

   b. Carrier identification (indicate if CG owned);

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

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

   e. Program supported;

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

g. Monthly recurring cost of the circuit.

2. Communication Area Master Station (CAMS) Distress & Safety Statistics. The Marine Information for Safety and Law Enforcement System (MISLE) does not capture distress and distress related safety communications relayed by the CAMS or COMMSTA Kodiak. Therefore, the 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-SAR) upon request to enable evaluation of system performance. Reports shall include:

a. Numbers of distress alerts received by medium frequency (MF)/HF voice, except those initiated by DSC;

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

c. Numbers of routine (non-safety related) calls received by MF/HF voice;

d. Numbers of distress alerts received by DSC, disregarding duplicate calls or relays of calls already received;

e. Number of DSC distress alerts for which there were follow-up communications by HF voice;

f. Number of DSC distress alerts for which there were no follow-up communications by HF voice;

g. Number of DSC distress alerts which did not include a position, or for which a position was obviously incorrect;

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

i. Numbers of safety or urgency calls received by DSC which resulted in follow-up voice communications; and

j. Number of DSC test calls received.

E. Daily Communication Logs.

1. General. Daily communication logs are official records, documenting communication and related events concerning the command. Communication logs also provide a record

that can be the subject of investigation or legal action. The two types of daily communication logs maintained are:

a. Complete Log. A manually completed (i.e., paper, electronic) or recorded (i.e. R21 system, DVL) log that contains all tactical and marine public safety communication data a unit transmits or receives. The following policy applies:

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

(2) Units with recording capabilities (i.e., R21 system, DVL) shall maintain a manual complete log (paper or electronic) only when the recording capability is inoperable; and

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

b. Abbreviated Log. An electronic or handwritten log that contains a synopsis of all tactical and maritime public safety communication data a unit transmits or receives. Verbatim entries are not required. The following policy applies:

(1) Units with recording capabilities (i.e., R21 system, DVL) shall maintain an abbreviated log;

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

(3) Units shall hold quarterly training on maintaining a complete manual log in the event of a recorder casualty.

2. Communication Log Requirements. Daily communication logs shall be maintained for all operational units, including CG Auxiliary and contingency communication assets, with the following exceptions:

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

b. Vessels under 65 feet in length;

c. Aircraft, except when acting as on-scene commander;

d. Unit vehicles with installed communications equipment; and

e. Personnel deployed with handheld communications equipment.

3. Daily Communication Log Content. The following information, at a minimum, shall be identified in communication logs:

   a. Unit name (use record message plain language address (PLA));

   b. Call sign;

   c. Date and time (Coordinated Universal Time (UTC), expressed as ZULU);

   d. Frequency/channel;

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

   f. Communications equipment status.

4. Daily Communication Log Policy. The following section provides additional policy for daily communication logs.

   a. Communication Log, Form CG-2614A, is available in the CG forms library. Use of this form is not mandatory. Units using other means for daily communication logs shall meet the minimum communication log content requirements established in section E.3 of this Chapter.

   b. Electronic or handwritten log entries shall not be erased.

   c. If handwritten, all entries shall be in blue or black ink.

   d. Changes to electronic or handwritten logs shall be made by drawing a single line in ink or typing slant signs through the original statement. The new entry shall be made adjacent to the original entry.

   e. All changes to the electronic or handwritten communication log shall be initialed in ink.

   f. 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.

   g. Use standard acronyms, abbreviations, designators, symbols, and signals appearing in official publications (e.g., ACPs, NTPs, and ITU publications) are authorized.

   h. Units shall log all distress, urgency, or safety signals and related communications, regardless of the type of log maintained. Ensure abbreviated log entries for distress, MEDICOs, and urgent signals contain the originator, frequency, time, and a brief

synopsis of what occurred. The log can make reference to the recorded log for more information, as required. Events shall be logged until it is apparent the unit will not participate in the assistance (e.g., outside AOR).

i. Units shall include cell phone communications in the daily communication log when the cell phone conversation pertains to distress, urgency, safety signals, and related communication.

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

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

5. Communication Area Master Station (CAMS)/Communication Station (COMMSTA) Kodiak/Air Station (AIRSTA) Kodiak Communication Logs. Radio Logs (RADLOGS) is a software logging program used at the CAMS and COMMSTA Kodiak. AIRSTA Kodiak has a single component of RADLOGS called Electronic Status Board. Units equipped with RADLOGS shall follow the log keeping policy of this Chapter when applicable. RADLOGS meets the abbreviated log requirement for units with recording devices.

F. Retention of Files, Reports, Records, and Logs. Reference (u) prescribes policies and procedures for administering CG Records, Forms and Reports Program as pertaining to the lifecycle management of both paper and electronic documents. The retention of telecommunication documents is provided in the following section.

1. Incidents of National Significance. Permanent retention, except as noted in paragraph c. Communication records qualifying for permanent retention shall be maintained at the unit that prosecuted the case or incident for three years and then transferred to a Federal Records Center (FRC) as outlined in Reference (u). These records include incidents or cases identified as having historical significance due to the scope or nature of the case, or cases involving prominent persons. Examples include:

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

b. Cases receiving national or regional media attention;

c. Cases used in Congressional or other oversight investigations;

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

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

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

2. Communication Records Directly Relating to Outstanding Exception, Claim, Litigation, or Investigation. Communication records directly relating to an outstanding exception by the Government Accounting Office, an outstanding claim for or against the United States, a case under litigation, or an incomplete investigation, shall not be destroyed until final clearance or settlement is determined. In addition, the following guidelines apply:

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

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

3. Search and Rescue (SAR) Case Files. Historically significant SAR cases (those having historical significance due to the scope or nature of the case, or cases involving prominent persons) are retained permanently and shall be forwarded to Commandant (CG-092). All other SAR case communication records can be destroyed 10 years after final closing of the case.

4. Audio Files. Audio files consist of recorded radio transmissions and telephone calls. Audio files shall be retained for 30 days, unless the audio file meets the retention requirements in sections F.1 through F.3 of this Chapter. The R21 system automatically stores a minimum of 30 days of audio files on the hard drive.

5. Joint Spectrum Interference Report (JSIR) – Report of Radio Interference. JSIRs shall be retained for 3 years.

6. Report of Violation of Radio Regulations or Communication Instructions, Form CG-2861A. All violation reports shall be retained for 3 years from the date of the incident.

7. Record Messages. Record messages shall be retained at the CAMS for 90 days. The following exceptions apply:

   a. CG Originated Record Messages. The originating office and action office shall retain the record message (paper or electronic) for a minimum of 90 days or until the information contained in the record message is no longer effective;

   b. General Record Messages. CG/ DOD/ Department of the Navy (DON) generated general record messages shall be maintained by the CAMS for 1 year after the date of promulgation;

c. Address Indicating Group (AIG)/Collective Address Designator (CAD) Promulgation, Modification, or Recapitulation Record Messages. CG generated AIG or CAD promulgation, modification, or recapitulation record message, and all those generated by DOD/DON used by CG units, shall be maintained by the CAMS until cancelled by the promulgating authority;

d. Record Message Tracer File. Retain for 6 months following resolution; and

e. High-Precedence Message Test Results. Retain for 1 year.

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

9. Administrative and Non-Essential Communication Records. Retained for 90 days.

10. Telecommunications General Files (Standard Subject Indicator Code (SSIC) 2000-2999). Includes plans, reports, and other records pertaining to equipment requests and telecommunication service. Retain for 3 years.

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

12. 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.

G. Disposal of Files, Reports, Records, and Logs. All communication files, reports, records, and logs can be destroyed without report (i.e. burning, shredding), if the following criterion is met:

1. Documents do not require transfer to the FRC; and

2. Documents meet the specified retention requirements per this Manual and Reference (u).

H. Telecommunication Inspections. Area, district, and sector commanders shall inspect their subordinate radio communication equipped units biennially. A checklist for the telecommunication inspection shall be included in the area Annex K to Area OPLAN and district supplements. The following guidelines apply:

1. Purpose. The primary purpose of the inspection is to evaluate the unit's ability to fulfill its telecommunication responsibilities. Exercise all telecommunication systems and contingency procedures during the visit whenever possible.

2. Pre-Brief/Post-Brief. A pre-brief shall be held prior to commencing the telecommunication inspection to provide the command with the visit purpose. Upon

completion of the telecommunication inspection, a post-brief shall be held to discuss the inspection outcome. A written report shall be provided to the command following the guidelines of section H.3 of this Chapter. The commanding officer or appointed representative from the command being inspected shall be present during both briefs.

3. Inspection Reports. The inspecting command shall forward a written report of the visit findings within 30 days of the inspection to the area C4IT division, unit commanding officer, and Commandant (CG-64 and CG-65). Units shall have 90 days for receipt of the written report to complete and document corrective/follow-up action. The following guidelines shall be followed:

   a. Note all deficiencies and inoperative systems; and

   b. Include follow-up action recommended and the responsible office tasked with the follow-up action.

4. Tracking. The area C4IT and district telecommunication division shall be responsible for tracking inspection schedules, the report, and response timeframes.

I. Destruction Devices. Information on selecting the correct destruction device for classified information, and the approved destruction methods, can be found in Reference (n). In addition,

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

   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.

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

   1. 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 per Reference (h) for vessels, including foreign vessels in United States SAR areas of responsibility, that:

      a. Deliberately transmit false alerts;

b. Inadvertently transmit a false distress alert without proper cancellation;

c. Fail to respond to a distress alert due to misuse or negligence;

d. Repeatedly transmit false alerts; and

e. Transmit distress alert using false identity.

2. Foreign Ship Violations. Contact local FCC Field offices to determine if they handle radio violations from foreign ships. If so, submit violation reports to the FCC. If not, violation reports should be submitted per Reference (h).

3. False Alert Feedback Solicitations. The procedures for false alert feedback solicitations can be found in Reference (a).

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

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

a. Transmission quality, particularly the communication procedures;

b. Product quality, formats, and content; and

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

2. Program Description. The following section provides a description of the Broadcast Quality Control Monitoring Program.

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

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

c. All communication facilities making BNMs 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 the United States CG-National Weather Service Coordination-Liaison Working Group (UNCLOG) via the chain-of-command (see Chapter 11 for UNCLOG description). The following specific policy applies:

(1) NAVTEX, HF Simplex Teletype Over Radio (SITOR), HF Radiofax, Inmarsat SafetyNET, and MF/HF voice broadcasts shall be monitored continuously for quality by each CAMS and COMMSTA Kodiak; and

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

d. In addition, commanding officers of units that broadcast maritime safety information shall work with the regional base C4IT division to measure transmitter performance at least weekly. Such measurements shall include measurement and verification of transmitted power, voltage standing-wave ratio, carrier frequency, and where applicable mark/space tone placement, frequencies, and tolerances.

CHAPTER 7 COAST GUARD (CG) TELECOMMUNICATION SHORE FACILITIES AND CONTINGENCY COMMUNICATIONS

A. General. CGTS facilities include the ITOC, CAMS, deployable systems, CCs, AIRSTAs, and the Vessel Traffic Service (VTS). The following sections detail policies pertaining to the operation of CGTS facilities, contingency communications, and CGTS facility design.

B. Command, Control, Communications, Computers, and Information Technology Service Center (C4IT SC). See Chapter 1 of this Manual for the functions of the C4IT SC.

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 watch provides 24x7 monitoring of DGPS, Long Range Identification and Tracking, NAIS Interim Receive and Permanent Transceive, and the Navigation Information Service. NAVCEN provides the general public with maritime telecommunications information and services on the following web site: www.navcen.uscg.gov.

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

1. Organization. Communication Area Master Station Atlantic (CAMSLANT) and Communication Area Master Station Pacific (CAMSPAC) are under the OPCON and ADCON of LANTAREA (LANT-6) and PACAREA (PAC-6). CAMS provide rapid, reliable, secure or protected, and interoperable communications for CG operational commanders, other government agencies, and the maritime public.

2. Purpose. The commanding officer of CAMS is responsible for the organization, operation, and supervision of the unit. 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 emergency situations.

3. Communication Station (COMMSTA). COMMSTAs are subordinate units under the OPCON and ADCON of CAMS. With the exception of COMMSTA Kodiak, COMMSTA operations are remotely operated by the CAMS. Each COMMSTA is staffed with technicians that maintain and supervise the operation of the COMMSTA 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)	

4. Communication Area Master Station (CAMS) Services. The CAMS have specific telecommunication responsibilities vital to the CGTS. CG telecommunication services provided by the CAMS for CG units, government agencies, or the maritime public are detailed in the following section.

   a. Directory Services. CAMSLANT manages all CG record messaging AIGs and CADs and maintains the CG general record message files. See Reference (a) for further information on CAMSLANT record messaging responsibilities.

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

   c. High Frequency (HF) Automatic Link Establishment (ALE) Networks. The CAMS, COMMSTA Kodiak, districts, and sectors 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. The HF ALE capable systems are as follows:

      (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. COTHEN has coverage limitations and is not available in the Western Pacific and some regions in Alaska; and

      (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.

      Note: Specific guidance 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) Broadcast Notice to Mariners (BNM). CAMS and COMMSTA Kodiak shall broadcast urgent, safety, and scheduled notice to mariners, in addition to, weather and hydrographic information. Specific responsibilities and broadcast schedules shall be prescribed in the Annex K to Area OPLAN and unit SOPs. Schedules shall be made available to the general public via the NAVCEN's website. The following broadcast modes are conducted by CAMS and COMMSTA Kodiak:

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

(2) HF voice, 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, in addition to, CBP's COTHEN.

f. Military Satellite Communication (MILSATCOM) Networks. Different military satellites are used to provide coverage to each CAMS AOR. The MILSATCOM networks at each CAMS are listed in the following section.

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

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

(b) TIN. Data only (NECOS).

(c) IW Voice.

(d) 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) IW Voice.

g. Global Maritime Distress and Safety System (GMDSS). This includes 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 12 of this Manual for DSC and GMDSS operations and policy.

h. Communications Assist Team (CAT). CAT visits provide unit specific training to fleet communicators. A CAT visit is an assessment of the unit's communication operations; it is not a communication inspection. Units should schedule a CAT visit prior to Command Assessment of Readiness and Training (CART) in preparation for Tailored Annual Cutter Training (TACT)/Tailored Ships Training Availability (TSTA) or following extended yard periods or in the event of large crew turnover. A CAT visit is provided to the unit at no cost.

Note: For further information regarding CAT services contact the CAMS or refer to the LANTCOMMSYS/PACCOMMSYS series record messages.

i. Mobile and Deployable Contingency Communications. See section I of this Chapter.

5. Communication Area Master Station (CAMS) Back-Up Communication Area Master Station (CAMS) (CBUC). CAMSLANT and CAMSPAC have limited ability to transfer control of communications assets between the two units during emergencies or unscheduled outages.

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. The following policy applies:

a. 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 commanders; and

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 TACON of all CG and other agency assets in the sector's assigned AOR. Sectors are primarily responsible for communications within sea area A1. Since R21 is primarily a sector operation, the following applies:

a. Sector commanders shall designate a minimum of two personnel as local R21 system supervisors. The systems supervisors are responsible for R21 user interface configuration management and locally established user interface configurations within R21 for the sector and boat stations; and

b. The R21 physical or system configuration shall not be adjusted by sector personnel. Configuration changes to R21 are only authorized by the C3CEN Remote Mission Systems Product Line Manager. Configuration changes will be implemented via TCTOs.

3. Boat Station. CG boat stations operate VHF/FM low sites for local command and control of forces and logistics purposes.

4. Air Station (AIRSTA). CG AIRSTAs communicate with CG assets through either the AIRSTA communication equipment or through the respective area COMMSYS. Aircraft communication is normally conducted within UHF/VHF frequency range; some AIRSTAs have MILSATCOM capabilities where necessary to ensure flight safety. Access to communication capability shall be provided to enable each aircraft to operate safely and efficiently to its maximum radius of operation.

5. Vessel Traffic Service (VTS). The VTS provides active monitoring, information, and navigational advice for vessels in confined and busy waterways. The purpose of VTS is to decrease vessel congestion, reduce critical encounter situations, and prevent marine casualties that could result in environmental damage or loss of life. The following information applies to VTS:

a. VTS uses a variety of sensors to monitor vessel traffic within the VTS region (e.g., radar, AIS, closed circuit television). The addition of AIS, radar and other surveillance tools combined with computer-assisted tracking allows the VTS to actively manage vessel traffic;

b. VTS operates on a VHF-FM communications network; and

c. Transiting vessels make position reports to the VTS by radiotelephone if not AIS equipped and are then provided with accurate, complete, and timely navigational safety information.

F. Shore Facility Contingency Communications Plans (CCP). Shore facilities that maintain a communication or record message guard for other units shall have a CCP in place to address outages and casualties. For further information on CCP, see Chapter 4 and Reference (a).

G. Coast Guard (CG) Vessel Lost Communication. Shore stations that lose contact with a CG vessel for which they have the guard for, shall attempt to reestablish communication directly with the vessel or through another station. If no communication is established, lost

communication notifications shall be made. When communication is reestablished with the vessel, all alerted units shall be notified. Area and district commanders can publish additional policy for alert procedures in lost communication situations. Reference (a) contains sample lost communication procedures.

H. Coast Guard (CG) Aircraft Lost Communication. Shore stations that lose contact with an aircraft for which they have the guard for shall initiate the necessary actions to re-establish communication with the aircraft either directly or through another unit. Area and district commanders can publish additional policy for alert procedures in lost communication situations. 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. When communication is reestablished with the aircraft, all alerted units shall be notified. Reference (a) contains sample lost communication procedures.

I. Deployable Contingency Communications. The CAMS maintain the CG's contingency communications assets that can provide temporary communications capabilities in support of COOP and other emergent requirements. Requests for contingency services shall be submitted through the operational commander via the appropriate area/district as outlined in LANTCOMMSYS/PACCOMMSYS series record messages and district supplements.

J. Shore Unit Search and Rescue (SAR) Communications. The following section outlines the policy for SAR communication for shoreside units. See Chapter 12 for further general policy on CG SAR communication.

1. Digital Selective Calling (DSC) Guard Requirements. The following section outlines shoreside DSC guard requirements

a. CAMS and COMMSTA Kodiak shall guard 6 DSC frequencies: 4207.5 kHz, 6312.0 kHz, 8414.5 kHz, 12577.0 kHz, and 16804.5 kHz.

(1) The DSC system logs test calls on all frequencies but filters these test calls, except on 4 MHz. The 4 MHz frequency has the Automatic Test Call Answering (ATA) function enabled and automatically responds to all tests received. The ATA is not enabled on the other MF/HF DSC frequencies but test calls can still be manually answered.

(2) HF DSC equipped units are not required to answer tests on other frequencies and are discouraged from doing so.

b. CG sectors equipped with R21 shall guard VHF-FM Channel 70 (156.525 MHz). DSC test calls received via VHF are automatically answered by the R21 system and do not require operator intervention.

c. Designated CG shore stations shall maintain a continuous watch on VHF-FM Channel 70 (156.525 MHz).

2. High Frequency/Medium Frequency (HF/MF) Digital Selective Calling (DSC) Response Policy: Coast Guard (CG) Shore Units. DSC is unique in that distress communication is initiated by widely distributed digital data bursts, but all follow-up communication after initial acknowledgement are typically handled by voice communication. The following section is policy for operational shore units responding to HF and MF DSC distress alerts.

   a. ITU regulations require each unit that receives a DSC distress alert or distress relay to send an acknowledgment.

   b. Multiple units may respond to the DSC distress alert. It is critical that CG units communicate with one another and with the default SAR mission coordinator (SMC) to ensure role clarity during DSC case operations.

   c. Shore units receiving a DSC alert outside their AOR shall wait a short period of time to allow the responsible unit to acknowledge receipt of the distress. However, during this short period of time, units hearing the distress shall notify their operational commander/RCC and contact the sector/unit closest to the distress to ensure they are aware of and are responding to the distress.

   Note: Further information regarding SMC determination, delegation, and responsibilities can be found in Reference (c).

3. Very High Frequency-Frequency Modulation (VHF FM) Digital Selective Calling (DSC) Response Policy: Coast Guard (CG) Shore Units. The R21 system provides CG sectors with VHF FM DSC capability. Until CG units are equipped with this capability, notification of receipt of a VHF FM DSC distress call can be received by sectors, foreign RCCs, and from third parties (including CG cutters equipped with VHF FM DSC). The following section is policy for operational shore units responding to VHF DSC distress alerts.

   a. VHF FM radios equipped with DSC maintain a continuous radio guard on VHF FM Channel 70 (156.525 MHz), regardless of the channel selected manually on the front panel. When a DSC distress alert is received 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 (156.800 MHz). If the radio does not automatically shift to VHF-FM Channel 16 (156.800 MHz) then the operator shall manually shift the radio.

   b. VHF FM DSC distress alerts shall be considered the equivalent of a MAYDAY distress alert, and shall require the same level of response per Reference (c).

K. Other Coast Guard (CG) Shore Unit Radio Frequency Guard Requirements. The following section lists additional minimum frequency guard requirements for shoreside units. Further information about these frequencies and other radiotelephone frequencies used by CG shore units can be found in Chapter 12 of this Manual.

1. High Frequency (HF) 4125 kHz. 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 this frequency.

2. Very High Frequency-Frequency Modulated (VHF-FM) Channel 16 (156.800 MHz). 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.

L. Telecommunication Facility Design Requirements. A telecommunication 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 Reference (v), and Shore Facilities Standards Manual, COMDTINST 11012.9 (series). Additional guidance is provided in the following section.

1. Facility Security. References (n) and (r) 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 per Reference (i).

   a. Communication equipment necessary for the proficient operation of the telecommunication facility shall 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) shall 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 Reference (m). Contact the C4IT SC for current TEMPEST guidance.

2. Emergency Power at Shore Facilities. Normal redundancy in CG communication capabilities exist through the ability 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 CG Shore Infrastructure Logistics Center (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 period of 72 consecutive hours without refueling;

   b. The emergency power supply at all CG shore telecommunication 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, operations deck, or where communication equipment is located. 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 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. The power supply system at all telecommunication facilities shall be tested per Reference (v); and

   d. Additional information concerning maintenance of generators is contained in Reference (i).

CHAPTER 8 COAST GUARD (CG) VESSEL AND MOBILE UNIT TELECOMMUNICATION

A. General. All CG cutters (vessels 65' and greater in length), boats (vessels less than 65' in length), and mobile units shall follow the principles and forms of communication prescribed in this Chapter, Reference (a), pertinent ACPs, JANAPs, CG LANTAREA and PACAREA Instructions, FCC policy and ITU policies, treaties and agreements.

B. Vessel Bridge-to-Bridge Radiotelephone Act. 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. The following section contains further information about the 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 Vessel Bridge-to-Bridge Radiotelephone Act is applicable on navigable waters of the United States inside the boundary lines established in 46 C.F.R. Part 7. The following CG vessels shall participate:

   a. Cutters while operating upon the navigable waters of the United States; and

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

2. Interpretation. The Vessel Bridge-to-Bridge Radiotelephone Act regulations state bridge-to-bridge radiotelephone is for the "exclusive use of the master or person in charge of the vessel, or the person designated by the master or person in charge to pilot or direct the movement of the vessel." For CG policy, this can be the commanding officer, officer-in-charge, conning officer, officer-of-the-deck (if actually directing the movement of the CG vessel), coxswain, or licensed pilot. This function shall not be delegated to others. All bridge-to-bridge communications shall be conducted in the English language. The following further information applies:

   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. 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;

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

d. The bridge-to-bridge radiotelephone frequency shall only be used to transmit and confirm the intentions of the CG vessel and any other information necessary for safe navigation;

e. Inoperability of the bridge-to-bridge radiotelephone(s) is not sufficient cause for non-participation. A portable radio can be used as the bridge-to-bridge radiotelephone;

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

g. 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.

C. Shipboard Communication Watches.

1. General. The communication watch is a primary duty assigned to Operations Specialists (OS) afloat. Depending on the size, location, and mission of the CG cutter, the commanding officer is required to establish SOPs to implement communication watch requirements per the Cutter Organization Manual, COMDTINST M5400.16 (series). Unit communication SOPs are required to be approved by the commanding officer. At a minimum, Communication SOPs shall be reviewed and updated annually to remain current with unit operational requirements.

2. Coast Guard (CG) Cutter Communication Watch Requirements.

a. Billet Structure. The billet structure on CG cutters is determined by the personnel allowance list promulgated by Commandant (CG-833). Watch requirements for CG cutters shall be per the following guidelines:

(1) Three or more OSs/Communications Watchstander Qualified Personnel. Maintain a continuous communication watch while underway, at anchor, or moored where landline communication is not available.

(2) Two or fewer OSs/Communications Watchstander Qualified Personnel. 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 CG vessel of frequency guard requirements per Exhibit 8-1.

b. Inport Watch Requirements. To determine the type of inport watch required, the following applies:

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

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

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

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

D. Coast Guard (CG) Vessel Radio Frequency Guard Requirements.

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

a. If a CG vessel is not suitably manned, the operational commander shall be notified and corrective action initiated; and

b. CG vessels without an OS assigned are still required to maintain the minimum frequency guards per Exhibit 8-1.

2. Under special circumstances, the operational commander can 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.

Exhibit 8-1
Minimum Radio Frequency Guards on CG Vessels

Class	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
WHEC*	X	X	X	X	X	X
WAGB*		X	X	X	X	
WMEC*	X	X	X	X	X	X
WMEC Mature Class*	X	X	X	X	X	X
WIX*, WLB*		X	X	X	X	
WLM		X	X	X	X	
CG Vessels 110' and larger, except WLIC		X	X	X	X	X
CG Vessels under 110' and over 26'		X	X	X	X	X
CG Vessels under 26'	As Required by the operational commander					

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

E. Coast Guard (CG) Vessel Search and Rescue (SAR) Communication. See Chapter 12 for overall CG SAR communications policy. The following section is specific for CG vessel SAR communications.

1. Digital Selective Calling (DSC) Guard Requirements. For DSC guard requirements, see Exhibit 8-1.

2. Coast Guard (CG) Vessel Very High Frequency-Frequency Modulation (VHF-FM) Digital Selective Calling (DSC) Response Policy. The following section is the policy for responding to VHF-FM DSC initiated distress alerts for CG vessels equipped with VHF-FM DSC equipment. 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.

   a. When a DSC distress alert is received on VHF-FM Channel 70 (156.525 MHz), the radio will emit a loud audio alarm, which is the equivalent of a MAYDAY and shall be handled with the same level of response. The radio should automatically shift to

VHF-FM Channel 16 (156.800 MHz), but if the automatic shift does not occur, operators shall manually shift channels.

b. As soon as possible, the SMC/commanding officer/OINC (whichever is applicable for the CG vessel reporting requirements) shall be informed of the contents of the distress alert.

c. In areas where reliable VHF-FM DSC communications with one or more shore stations are known not to exist, CG vessels that receive a VHF-FM DSC distress alert shall, as soon as possible, notify the appropriate SCC and acknowledge receipt of the distress alert when instructed;

d. In areas where reliable VHF-FM DSC communications with one or more shore stations are feasible, the CO/OINC/coxswain (whichever is applicable for the CG vessel) shall defer acknowledgement so that a shore station can acknowledge receipt of a call. Any CG vessel receiving a call that is not acknowledged by a shore station within 5 minutes shall acknowledge the call using the following policy:

(1) Acknowledge receipt of the alert on VHF-FM Channel 16 (156.800 MHz) and attempt to establish communication with the distressed vessel;

(2) If unable to establish voice communication with the distressed vessel, CG vessels 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) CG Vessels that acknowledge receipt of DSC distress alerts are responsible for informing the applicable SCC or Rescue Coordination Center (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.

F. Coast Guard (CG) Cutter Communication. This section outlines the policy for cutter communications.

1. Operations Normal Reports. Operations normal reports shall be conducted per the operational commander. See section H of this Chapter for exemptions to Operations Normal Reports.

2. Communication Guard Shift (COMMSHIFT). COMMSHIFTs shall be submitted to transfer a telecommunication guard and record message delivery responsibility to another unit. COMMSHIFT record messages not submitted result in missed record

messages for the command. The procedures for submitting COMMSHIFT record messages are in Reference (a). The following policy applies:

a. 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;

b. Mobile units deploying for less than 72 hours are not required to submit COMMSHIFT record messages unless shifting to a USN unit; and

c. Command shall contact the appropriate guarding facility to ensure their submitted COMMSHIFT record message has been received prior to the COMMSHIFT taking effect.

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

4. Communication Guard List. The communication guard list is used by mobile units to determine record message guard requirements. Commanding officers shall be responsible for maintaining an accurate guard list for AIG, CAD, and task organization assignments. The following applies:

a. Cutters shall request and review their command's guard lists prior to deployment and update as necessary;

b. Ensure the applicable CAMS are an action addressee on all guard list requests, submittals, and modifications.

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

G. Coast Guard (CG) Boat Communication. Operations Normal reports are required for all boats per the Boat Crew Seamanship Manual, COMDTINST M16114.5 (series). See section H of this Chapter for exemptions to Operations Normal Reports. The following applies:

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

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

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

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

H. Exemptions to Operations Normal Reporting Requirements. CG vessels operating under the following conditions are exempted from operations normal report requirements:

1. When maintaining communication with the on-scene commander in conjunction with a SAR mission. A cutter/boat engaged in a SAR mission and reporting to an on-scene commander shall shift its telecommunication guard and reporting requirements to the on-scene commander until released from the SAR mission; or

2. When instructed by proper authority to maintain radio silence. In any case of planned radio silence, the shore facility shall be notified. Communication shall be re-established when authorized by the issuing authority.

I. Coast Guard (CG) Vessel Lost Communication. CG vessels losing contact with the guarding shore station must attempt to reestablish communication directly with the shore station or through another station. Area and district commanders can publish additional policy for alert procedures in lost communication situations. Lost communication procedures between a CG vessel and CG aircraft can be found in Shipboard-Helicopter Operational Procedures Manual, COMDTINST M3710.2 (series).

J. Visual Communication Policy. The following section provides policy for visual communication.

1. Visual Watch Requirements. The commanding officer or operational commander shall determine the need and assignment of personnel as visual communication watchstanders. Visual communication watchstanders shall be trained to use all forms of visual communication required, based on cutter requirements (e.g., flags, flashing light).

2. General Visual Policy. The following policy shall be followed for visual communication:

a. When the identity of a ship has been established as CG, USN, or as an allied naval vessel, the visual signaling procedures in Reference (w) shall be used.

b. The procedures for visual communication found in the International Code of Signals (INTERCO), National Geospatial-Intelligence Agency (NGA) Pub. 102, shall be

used when exchanging calls with ships of unknown registry, merchant ships, and non-allied ships. The prosigns in Reference (w) have a different meaning than the prosigns in NGA Pub 102.

3. Flashing Light. Directional flashing light is the transmission of signals by a narrow beam of light such as a signaling searchlight. To reduce the probability of interception, directional flashing light shall be the primary method of flashing light communication. Non-directional flashing light is the transmission of signals in all directions by a signal light, such as a yardarm blinker. Non-directional flashing light shall be considered the secondary means of flashing light communication, and can be used in situations where the signaling unit desires to signal more than one addressee at a time. The following flashing light policy applies:

   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; or

      (2) Use red or green filters with caution ; the intent is to not override or be mistaken for the sidelights of a ship when underway; and

   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 is an operating signal that translates to: "The following is to be taken as applying to personnel on watch only." Unofficial signaling shall only be conducted with authorization from the commanding officer or officer-in-charge.

4. Visual Communication Records. When maintaining a visual signal watch, all visual signals used for communications shall be entered into the unit communication log.

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

K. Coast Guard (CG) Mobile Unit Contingency Communications Plans (CCP). CG mobile units that maintain a communication or record message guard for other units shall have a CCP in place to address outages and casualties. For further information on CCPs, see Chapter 4 and Reference (a).

CHAPTER 9 COAST GUARD (CG) AIRCRAFT TELECOMMUNICATION

A. General. All CG aircraft shall follow the principles and forms of communication prescribed in this Manual, Reference (a), pertinent ACPs, JANAPs, CG LANTAREA and PACAREA instructions, International Civil Aviation Organization (ICAO), Federal Aviation Administration (FAA) publications, FCC policy and ITU policies, treaties and agreements. The following general guidance is provided:

1. An aeronautical facility is defined as a land station in the aeronautical mobile service and includes civilian air traffic controls, CG AIRSTAs, sectors, or other military facilities. If available, CG aircraft shall 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 (e.g., taxiing, fire/crash truck dispatch) shall be conducted on UHF-AM and/or VHF-FM over non-maritime mobile bands; and

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 are not normally approved.

B. Coast Guard (CG) Aircraft Communication Guard Policy. The following section outlines the communication guard policy for aircraft.

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

   a. 121.5 MHz;

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

   c. 243.0 MHz.

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

2. CG aircraft shall establish a communication guard with an aeronautical facility or CG facility within 5 minutes after takeoff.

3. The aeronautical facility 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. It is the responsibility of the aircraft commander to ensure the

communication guard unit at the point of departure or arrival is properly notified of the aircrafts movement.

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

5. The CG communication guard unit shall provide primary and secondary frequencies, the next scheduled communication check and following communication checks thereafter.

6. If a change of communication guard is necessary due to operations or deteriorating communications, the aircraft must ensure the communication guard unit is immediately notified via any means. Failure to do so can result in lost communications procedures being implemented and unnecessarily diversion of assets.

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

C. Coast Guard (CG) Aircraft Reporting Requirements. AIRSTAs normally receive medium and long range air-to-ground support from the area COMMSYS. The following section outlines aircraft reporting requirements.

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 with the following guidelines:

      (1) Normal flight operations status reports shall be transmitted as “flight ops normal”;

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

      (3) Position reports shall include true course, altitude and speed.

   b. Rotary - Helicopters. A flight operations status report every 15 minutes and a position report every 30 minutes with the following guidelines:

      (1) Normal flight operations status reports shall be transmitted as “flight ops normal”;

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

      (3) Position reports shall include true course, altitude and speed.

2. Any communication between an aircraft and the communication guard unit can be used to begin a new reporting period.

3. When the aircraft is maintaining communication with air traffic control facilities, the required reports shall be made per current FAA regulations. Whenever possible, the aircraft commander shall also maintain a guard on CG frequencies if it does not interfere with the primary air traffic control communication.

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

D. Coast Guard (CG) Aircraft Lost Communication. Aircraft commanders that lose communication with their guard unit shall initiate the necessary actions to re-establish communications with the guard unit either directly or through another unit. Area and district commanders can publish additional policy for alert procedures in lost communication situations. Reference (a) contains sample lost communication procedures.

E. Coast Guard (CG) Aircraft Frequency Selection. 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/. The following section outlines additional policy pertaining to CG aircraft frequency selection.

1. 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 carrier frequency 4125 kHz or on the carrier frequency VHF-FM Channel 16 (156.800 MHz).

   Note: The safety of life and non-interference exceptions is at the determination of the pilot. In making this determination, the pilot 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 can include transmissions on channels exclusively allocated to the CG (i.e., VHF-FM Channel 21A (157.050 MHz), VHF-FM Channel 23A (157.150 MHz), VHF-FM Channel 83A (157.175 MHz)) provided that propagation does not overlap any foreign national waters absent permission from that government and that all affected sectors are aware of the operation.

2. 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 can be used to communicate with CG boats and sector shore units. The following applies:

a. In emergencies or SAR situations CG aircraft can 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 per Reference (h);

b. VHF-FM Channel 83A (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 can 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 can operate on these channels up to an altitude 1500 feet. The following additional information applies:

   (1) Transmissions by aircraft in this band shall not exceed 5 watts; and

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

e. 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; and

f. Aircraft can broadcast urgent maritime safety information and weather warnings to ships. The following additional information applies:

   (1) District commanders shall determine policy on broadcast content and when such broadcasts are necessary;

   (2) 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;

(3) Transmission duration on VHF-FM Channel 16 (156.800 MHz) shall be short and in no cases exceed 1 minute;

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

(5) Appropriate sector watchstanders and foreign RCCs shall be notified, where appropriate, before commencement of broadcasts.

3. High Frequency (HF). CG HF air-to-ground frequencies shall be used for long range communication with a CAMS or COMMSTA Kodiak. The following HF networks are available for CG aviation use:

a. Secure Air-to-Ground (SAG). SAG is a secure 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; and

c. Geo-Spatial over the Horizon ALE Matrix (GOTHAM). COMMSTA Kodiak operates GOTHAM to provide both clear and secure aircraft communication.

F. Digital Selective Calling (DSC). CG aircraft equipped with VHF FM DSC radios shall guard DSC VHF-FM Channel 70 (156.525 MHz). CG aircraft in receipt of an urgent DSC alert shall immediately relay the pertinent information to their operational commander via the most expeditious means available, if operations permit. Further general policy regarding CG SAR communication can be found in Chapter 12 of this Manual.

G. Radio Silence. When the aircraft has been instructed by proper authority to maintain radio silence, the following applies:

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

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

H. Coast Guard (CG) Aircraft Voice Call Signs. Voice call signs for aircraft shall be per Reference (x) 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.

I. RT-5000 Very High Frequency/Ultra High Frequency (VHF/UHF) Code Plugs. For information on the RT 5000 VHF/UHF code plugs, see Chapter 4 of this Manual.

CHAPTER 10 COAST GUARD (CG) AUXILIARY TELECOMMUNICATION

A. General. The CG Auxiliary has long been a valuable contributor to the success of the overall CG mission. Subsequent to the events of September 11, 2001 and the increasing focus by the CG on the Homeland Security mission, the contributions of the CG Auxiliary have taken on new importance. This Chapter discusses the policy for CG Auxiliary communications and the criticality of protecting operational communications for all CG assets involved in Homeland Security and law enforcement missions.

B. Coast Guard (CG) Auxiliary Communications Network. The CAMS are responsible for control of the CG Auxiliary communication network. This includes providing CG Auxiliary personnel training and drills. The area commander, district commander, CAMS or Commandant (CG-65) shall designate frequencies authorized for CG Auxiliary use. Authorized use of the designated frequencies shall be for contingency communications, COOP, quality control, regattas, and other Auxiliary official events.

C. Coast Guard (CG) Auxiliary Communication Policy. The following section outlines policy for CG Auxiliary communications. Further information regarding Auxiliary communications and operations can be found in the Auxiliary Operations Policy Manual, COMDTINST M16798.3 (series).

1. Keyed Very High Frequency-Frequency Modulated (VHF-FM) and Ultra High Frequency (UHF) Handheld Radios. CG Auxiliary personnel are authorized to use SBU keyed VHF-FM and UHF handheld radios to support CG operations.

2. CG Auxiliary Handheld Radio Issuance. Units are authorized to issue keyed handheld radios to CG Auxiliary personnel. The unit shall ensure the following prior to issuing the keyed handheld radio:

   a. The CG Auxiliary member is qualified as CG Auxiliary communications operator per local unit requirements;

   b. The CG Auxiliary member has a favorable operational support personnel security investigation and has a signed COMSEC Material System (CMS) User Acknowledgement Form on file;

   c. The CG Auxiliary member has a signed non-disclosure agreement (DHS Form 11000-6) on file;

   d. The CG Auxiliary member has a letter on file signed by the CG orders issuing authority authorizing use, possession and custody of keyed handheld radios; and

   e. The CG Auxiliary member has completed unit training in keyed radio operations, storage, transportation, reporting loss/stolen keyed radios, and OTAR capabilities/operation.

3. Coast Guard (CG) Auxiliary Handheld Radio Use. CG Auxiliary personnel shall:

   a. Operate the radio only while under CG orders;

   b. Operate keyed radios per approved Annex K to Area OPLAN district supplement and local SOPs;

   c. Not maintain custody of physical cryptographic KEYMAT or physical loading devices; and

   d. Not maintain personal custody of keyed radios unless specifically authorized to do so by higher authority.

4. Cryptographic Keying Material (KEYMAT) Loads. The following policy applies to the cryptographci KEYMAT load of CG Auxiliary handheld radios:

   a. The loading of cryptographic KEYMAT in radios distributed to CG Auxiliary personnel shall be limited to authorized CG personnel at the CG unit to which assigned or at an authorized CG support unit; and

   b. Authorization to load cryptographic KEYMAT can be assigned to another CG unit on a limited case-by-case basis only.

5. Telephony Policy. Per Chapter 3 of this Manual, Auxiliary members are not authorized federal calling cards or the use of DSN services.

6. Broadcast Quality Control Monitoring Program. Area commanders shall engage the CG Auxiliary where appropriate to assist in broadcast quality control monitoring efforts. This engagement shall be initiated and managed through the Auxiliary Department of Operations Telecommunications Division at the national level (AUX-DVC-OT) who shall designate an Auxiliary command POC for the CAMS. See Chapter 6 of this Manual for further information on this program.

CHAPTER 11 COAST GUARD (CG) PUBLIC MARITIME BROADCAST OPERATIONS

A. General. Per 33 C.F.R. 72.01-25, the CG is authorized to broadcast notice to mariners on its own. Distress, urgent, and safety broadcasts are made as required, along with regularly scheduled marine safety information broadcasts. A BNM is the method by which important navigation safety information is disseminated in the most expedient manner. In general, these broadcasts 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.

B. United States Coast Guard (CG)-National Weather Service Coordination-Liaison Working Group (UNCLOG). UNCLOG is responsible for the configuration management of NOAA's NWS text and graphic products to be broadcast by CG telecommunication facilities. Record message formatting requirements for BNM of any type are included in Reference (y). 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.

C. Vessels Subject to the Safety of Life at Sea (SOLAS) Convention. SOLAS vessels do not 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:

1. DSC All-Ships urgent or safety priority calls are authorized on VHF-FM only. On MF/HF, an urgent or safety call must be addressed to a specific ship or to a specified geographical area. An All-Ships call is not allowed on MF/HF.

2. 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;

3. 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; and

4. The ITU sector for Radiocommunications indicates excessive test calls on MF/HF DSC distress and safety frequencies overloads the system to the point where interference to distress and safety calls has become a cause for concern. To minimize possible interference, live testing on DSC distress and safety frequencies with coast stations should be limited to once a week as recommended by IMO.

D. Broadcast Notice To Mariners (BNM) Types.

1. Urgent Marine Information Broadcast (UMIB). Urgent broadcasts concern the safety of a ship, aircraft, other vehicle, or the safety of a person. Urgent broadcasts shall be used

to announce severe weather (e.g., hurricanes, hurricane force winds, tsunami warnings) and issues regarding safety of life at sea.

2. Safety Broadcast Notice to Mariners/ Safety Marine Information Broadcast (SMIB). Safety broadcasts contain important navigational and meteorological warnings, sunspot activity, or other unusual events that might impact maritime activities. The safety signal shall precede a safety broadcast. Safety 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 broadcast shall normally consist of only one subject. The following section provides further information on safety broadcasts.

   a. Weather Warnings. Weather warnings are transmitted upon receipt as a safety broadcast on MF, and from all VHF FM sites identified in the "National Weather Service Products Recommended for Broadcast", (link provided in section B of this Chapter).

      (1) 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 can be decided by UNCLOG. Any proposed changes shall be submitted through district or area C4IT staff.

      (2) The area commander can 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.

   b. Navigational Warnings. Navigation information is the manner in which the Coast Guard keeps mariners aware of important safety information such as changes to aids to navigation, hazards, channel depths and conditions, and corrective information for charts and publications. Navigation information is primarily disseminated in the form of local notices to mariners, light list, and BNMs. The BNM shall be broadcast per the broadcast instructions contained in the record message. Cutters requiring this navigational information via record message shall contact LANTAREA (LANT-3) or PACAREA (PAC-3) for guidance.

3. Scheduled Broadcast Notice to Mariners. Scheduled BNMs include search and rescue, navigational, hydrographic, or weather information. In addition,

   a. Safety and urgent record messages that remain in effect at the next scheduled broadcast shall be repeated;

   b. Area and district commanders shall coordinate their broadcast times to minimize interference problems;

c. HF, MF, and VHF-FM broadcasts shall be scheduled so that no interference occurs in overlapping coverage areas;

d. 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; and

e. Area commanders shall publish scheduled BNM content and broadcast times for each broadcast station in their Annex K to Area OPLAN. Any proposed changes shall be submitted through the area C4IT or district telecommunication division.

E. Broadcast Notice to Mariners (BNM) Duration. The textual length of record messages for the BNM broadcast shall be kept to a minimum consistent with the need to pass important information. Urgent information and other warnings can be broadcast on international distress and calling frequencies (VHF FM Channel 16 (156.800 MHz)) provided the broadcast does not exceed one minute. An appropriate working frequency shall be used for broadcasts requiring more time for transmission.

F. Broadcast Notice to Mariners (BNM) Originator Responsibilities. This section covers the originators responsibilities for the development, review and cancellation of BNMs.

1. Format. The BNM originator shall use the subject lines and readily recognizable abbreviations per Reference (y). In order to use the NAVTEX system as a broadcast alternative, BNM originators shall ensure all types of broadcasts are formatted the same to alleviate the need to re-key the NAVTEX transmission. An exception to this, if broadcasting NWS information, operators shall transmit the exact text received from the NWS.

2. Reviews. Originators of broadcasts shall review their active BNMs including broadcasts made by the NGA at CG request daily to avoid transmitting duplicate or outdated information.

G. Broadcast Cancellations. It is the responsibility of the originator to cancel broadcast record messages once action is no longer necessary. Originators shall provide a cancellation date on BNMs where possible.

1. A cancellation record message shall be sent for any BNM without a cancellation date.

2. Originators shall issue weekly summaries of all active BNMs per Reference (y).

H. General Broadcast Guidelines. The following guidelines shall be followed in the performance of public maritime broadcast operations:

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, forecast winds.) sent at reduced rate/speed to enable listeners to copy this information. Proper diction is essential and the text shall be read in phrases rather than word by word; and

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

I. Broadcast Notice to Mariners (BNM) Service Changes and Casualties. It is essential that the CG notify the maritime community of changes or outages in distress, safety, and broadcast operations. The following section provides further policy on BNM service changes and casualties.

1. Changes, casualties, and casualty corrections concerning the following services shall be sent to the applicable CG broadcast station for broadcast as a BNM per Reference (y):

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

   b. VHF-FM Channel 22A (157.1 MHz);

   c. District CC and SCC emergency telephone; and

   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 navigational area (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. HF Single sideband voice GMDSS guards; and

   d. Area CC emergency telephone and telex numbers.

3. For outages that impact district and area CCs, the following shall be notified:

a. Vizada via e-mail (https://sby2.vizada-usa.net/ttlink/term/ccare.jsp) Southbury, CT Teleport (shift leader +1-203-262-5010)

b. Inmarsat London UK
011-44-0-20-7728-1142

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

J. Navigational Telex (NAVTEX).

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

a. CG CCs 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 uses this system as a means of disseminating ice bulletins and warning messages; and

c. Districts, sectors, and NAVCEN use this system as a means of disseminating BNMs.

2. Administration. NAVTEX policy is administered by the IMO's International NAVTEX Coordinating Panel. Commandant (CG-652) is the national NAVTEX coordinator. Area commanders are the NAVTEX coordinators for the CG, and shall ensure broadcasts are reliable, on schedule, within the prescribed duration, and practicable without interference.

3. Operational Requirements. The NAVTEX operational requirements are described in NAVTEX Manual, International Maritime Organization MSC Circular 416.

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

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); and

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. Broadcast Schedule. The following section applies to CG NAVTEX broadcasts.

a. CG NAVTEX broadcasts are conducted six times daily per the following policy:

(1) All six scheduled broadcasts have navigational warnings, if required;

(2) BNMs shall be broadcasted for the period designated by the originator; and

(3) Repeats of BNMs shall be moved to the two daily broadcast slots where weather is not normally broadcast

b. Although IMO limits NAVTEX broadcast duration to 10 minutes, the CG is authorized a 20 minute transmit duration due to greater than normal site separation in the United States. The maximum duration of a NAVTEX broadcast is 40 minutes. Broadcasts can exceed this 40 minute limit if there is no other station in the area scheduled for that period, or if the station scheduled for that period gives permission to continue broadcasting. Additionally, the following policy applies:

(1) If broadcast is expected to exceed 40 minutes, all new messages shall be transmitted during the first 40 minutes; and

(2) 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, but before repeated messages.

c. Messages are sent in the order received and in order of priority. All new messages shall be transmitted before old messages received but not before previously broadcast messages. Messages broadcast during the previous schedule shall be broadcast at the end of the broadcast.

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

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

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

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

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

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

K. Summary of Radiotelephone and Navigational Telex (NAVTEX) Broadcast Requirements. NAVTEX broadcast scheduling guidance are provided in Exhibits 11-1, 11-2, and 11-3.

Exhibit 11-1
Atlantic Area NAVTEX Broadcast Schedules

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

Exhibit 11-2
Pacific Area NAVTEX Broadcast Schedules

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

Exhibit 11-3
Radiotelephone/NAVTEX Broadcast Requirements

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

A: Upon receipt,
B: Every 15 minutes for a 1 hour period.
C: Repeat next scheduled broadcast, unless 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.
Note 1: Broadcast on 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.

L. Additional 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. These additional automated broadcasts are described in the following section.

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 is used to broadcast marine safety information including high seas forecasts, NAVAREA warnings, ice, and hydrographic

information in hard copy form. Currently only CAMSPAC (including Guam) and COMMSTA Boston provide this service to the public.

3. Radio Facsimile (Radiofax). Radiofax is a service of the NWS that is broadcast from CG CAMS and COMMSTA Kodiak. Radiofax automation is a function of NWS. Radiofax products are traditional weather charts for specific geographic areas.

M. Inmarsat All-Ships Search and Rescue Broadcasts. Shore-to-ship distress and search and rescue broadcasts can be made at no charge to all Inmarsat equipped ships in a particular Inmarsat ocean region. Broadcasts shall be limited to those cases involving grave and imminent danger.

N. Other Broadcasting Systems. Units that broadcast information via radio, cellular, and data circuits other than those listed in this Manual shall conform to the policies and standards for content and timeliness provided in this Manual and other applicable SAR and ATON references.

O. Broadcast Quality Control Monitoring Program. See Chapter 6 of this Manual for further information on this program.

CHAPTER 12 COAST GUARD (CG) SEARCH AND RESCUE (SAR) TELECOMMUNICATION

A. General. A primary function performed by CG telecommunication personnel is to provide rapid and reliable communication to vessels in distress. 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. This Chapter outlines the policy for CG telecommunication during SAR missions. The following guidance applies:

1. Under 14 U.S.C § 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; and

2. CG personnel involved with SAR responsibilities shall adhere to current procedures described in Reference (c), Communications Instructions Distress and Rescue Procedures, ACP 135 (series), and ITU Radio Regulations.

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

1. Rescue Coordination Center (RCC) and Command Center (CC). RCC and CC responsibilities and geographic locations can be found in Reference (c).

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. All communications destined for the cognizant RCC or CC shall be via the on-scene commander. Procedures for coordinating SAR telecommunication are in Reference (a).

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. In addition, area and district commanders shall ensure:

   a. Assignment of continuous radio watches on distress frequencies by as many units as necessary to provide adequate AOR coverage. See Chapters 7, 8, and 9 of this Manual for specific frequency guard requirements for CG shore facilities, vessels and aircraft;

b. All units proactively respond to all distress calls received and ensure the call is relayed to the appropriate CC/RCC; and

c. Prompt broadcast of distress information, per current laws and privacy policies, to the maritime public, who can be capable of providing assistance. The following guidelines shall be adhered to:

(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; and

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

C. Distress Communication Policy. The following section provides policy for distress communication.

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. In addition:

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;

b. No transmissions shall interfere with distress traffic; and

c. Since a distress call is not addressed to a particular station, an 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 free assistance and medical advice to seamen from all over the world via radio. MEDICOs and medical evacuations are part of the traditional CG SAR mission. All MEDICO messages are a potential assistance case and of interest to the CG. The CG provides message relay services for CIRM. The CG is not acting as a government agency responsible for providing free medical message service. Instead, the CG radio facilities are used free of charge in the same manner as commercial facilities for this type of service. NGA's Radio Navigational Aids, Pub 117 (series) and ITU's "List of Coast Stations and Special Service Stations (List IV)" contain commercial and government radio stations that provide free medical message services to ships. Deadhead (DH) MEDICO (non-chargeable medical

message) message procedures are contained in Reference (a). The following policy applies:

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. RCCs and SCCs shall establish procedures for consultation with medical facilities or CG assigned Public Health Service medical doctors;

c. Area CCs shall have local procedures in place for handling incorrectly addressed DH MEDICO messages;

d. In the event a medical case develops a need for CG assistance, the messages shall be handled by 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 CC shall send a DH MEDICO message chargeable to the CG via commercial facilities; and

e. CCs shall maintain liaison with commercial facilities to ensure the CG remains well informed regarding MEDICO messages not handled via CG circuits.

3. Medical Communication. For the purpose of announcing and identifying medical transports 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).

4. Initial Search and Rescue (SAR) Check Sheet. Communications watchstanders shall use an initial SAR check sheet for all SAR related reports. An example of an Initial SAR Check Sheet is contained in Reference (c).

5. Distress Electronic Mail (Email) and Text Messaging Policy. Some communication providers have email and text messaging capabilities. Email and text messaging are not designed for distress communication; therefore, the CG does not endorse use of either service for distress alerting purposes. Additional information regarding distress email and text messaging is contained in Reference (c).

6. Telephone Policy. The commanding officer or officer-in-charge of each unit shall ensure personnel are proficient in handling telephone calls of a distress nature before assigning them to duty answering telephones. In addition, if the CG unit cannot take action in response to a distress call the commanding officer or officer-in-charge shall ensure personnel know how to relay the information to appropriate supervisors or authorities.

7. Distress Cellular Telephone Policy. Marine cellular telephone usage 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 a VHF-FM radio. In addition,

    a. A voice call made via cellular telephone can be recorded on the SCC's DVL as long as the call is made to a distress telephone line. When properly used, cellular phones meet the requirements of reliable communication as outlined in Reference (c). Cellular telephone communications are point-to-point. Cellular telephone conversations cannot be heard by other boaters in the area who may be in a position to render immediate aid to someone in distress; and

    b. When a distress call is received via cell phone and the caller's location is not known, use the procedures outlined in Reference (a) to determine the location of the caller.

D. Very High Frequency (VHF) Communication Policy. VHF-FM systems are the preferred and most effective method of voice communication in sea area A1. 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 Reference (a), for specific R21 system operating procedures. The following section provides policy on VHF communication.

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. In addition,

    a. If the two systems provide un-resolvable conflicting information, use both data sets for case analysis in search planning; and

    b. Until each sector accepts R21, 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. The following section outlines policy for R21 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.

E. Global Maritime Distress and Safety System (GMDSS). GMDSS is an international system that uses terrestrial and satellite technology, along with ship-board radio systems, to ensure rapid, automated alerting of shore-based communication and rescue authorities, in addition to ships in the immediate vicinity, for maritime distress events. Further GMDSS information is in the following section.

1. Applicability to Commercial Vessels.

a. GMDSS equipment requirements are mandatory for vessels subject to the Safety of Life at Sea (SOLAS) Convention of 1974.

b. All cargo vessels 300 gross registered tons and up, and all passenger ships engaged in international voyages, must be equipped with GMDSS systems that meet international standards.

2. Global Maritime Distress and Safety System (GMDSS) Coverage Areas. GMDSS divides the world's oceans into four sea areas. SOLAS ships have distinct equipment carriage requirements for each area through which they transit:

a. Sea Area A1. An area within the radiotelephone coverage of at least one VHF-FM coast station in which continuous DSC (VHF-FM Channel 70 (156.525 MHz)) alerting and VHF-FM Channel 16 (156.800 MHz) radiotelephony services are available, as defined by the IMO. Sea area A1 covers the area from the coastal area up to approximately 20 nautical miles offshore.

b. Sea Area A2. An area within the radiotelephone coverage of at least one MF coast station (excluding sea area Al) in which continuous DSC (2187.5 kHz) alerting and 2182 kHz radiotelephony services are available, as defined by the IMO. GMDSS-regulated ships traveling this area must carry a DSC-equipped MF radiotelephone in addition to equipment required for sea area A1. Sea area A2 covers the area from the coastal area up to approximately 200 nautical miles offshore. The CG has declared it does not provide coverage in Sea Area A2.

c. 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.

d. Sea Area A4. The remaining sea areas outside sea areas A1, A2, and A3 (i.e., Polar Regions). Ships traveling this area must carry a DSC-equipped HF radiotelephone/telex, in addition to equipment required for sea areas A1 and A2.

3. Distress Alerting Methods. 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.

4. General Global Maritime Distress and Safety System (GMDSS) Policy. The following section provides GMDSS policy.

   a. Harmful Interference. Any emission causing harmful interference to distress and safety communication on any of the discreet GMDSS frequencies is prohibited. Before transmitting on a GMDSS frequency for any purpose other than distress, a station shall listen on the frequency to ensure no distress transmission is being sent.

   b. Test Transmissions. For GMDSS frequencies, the number and duration of test transmissions shall be kept to a minimum. Test transmissions shall be coordinated with a competent authority, and carried out on artificial antennas or with reduced power when possible. For distress and safety calling frequencies, test transmissions should be avoided; however, if unavoidable, a test transmission announcement shall be made on that frequency.

   c. Survival Craft. Radiotelephone equipment installed in survival craft that operates in the frequency range of 156 MHz to 174 MHz, shall have the capability to transmit and receive on VHF-FM Channel 16 (156.800 MHz) and at least one other frequency in that range.

   d. Distress Traffic. Distress traffic consists of all messages relating to the immediate assistance required by the ship in distress, including search and rescue communication and on-scene communication. For distress traffic by radiotelephony procedures, refer to Reference (x). The following policy applies:

      (1) 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 mode (forward error correction (FEC)). If advantageous, the automatic repeat request (ARQ) mode can be used subsequently;

      (2) The CC responsible for coordinating SAR operations shall manage distress traffic relating to the incident or appoint this responsibility to another station. In addition,

(a) If a station interferes with distress traffic, silence can be imposed by the following: the RCC coordinating distress traffic, the unit coordinating SAR operations, or the coast station involved with the distress. Silence imposition can be addressed to either all stations or to only a single station. In narrow-band direct-printing telegraphy normally using FEC, the signal SILENCE MAYDAY. However, the ARQ mode can be used when it is advantageous to do so; and

(b) When the distress situation concludes, the CC controlling a SAR operation shall initiate a message for transmission on the distress traffic frequencies indicating the distress traffic has ceased.

(3) On-scene communication is defined as: (1) the communication between the vessel in distress and the assisting response units, and (2) the communication between the response units and the unit coordinating SAR operations. The unit coordinating SAR operations shall have control of on-scene communications.

e. Transmission of Maritime Safety Information. These transmissions shall be preceded by the safety signal.

5. Global Maritime Distress and Safety System (GMDSS) Sub-Systems. GMDSS consists of numerous telecommunication sub-systems, including:

a. Digital Selective Calling (DSC). Used for distress, urgency, safety, routine, ships business, and test calling via HF, MF, and VHF-FM. DSC is digital technology intended to initiate non-voice communication over maritime radio and provide distress alert information to CG CCs and foreign RCCs. The following section provides further DSC policy and capabilities.

(1) General. The following section provides additional information for DSC use.

(a) DSC distress calls are electronically relayed to the CG by any vessel that has a DSC compatible radio.

(b) DSC calls use the applicable MMSI number and appropriate DSC guard or calling frequencies. Mariners can instantly send an automatically formatted distress alert to the CG or other rescue authority anywhere in the world.

(c) Mariners can initiate or receive distress, urgency, safety, and routine radiotelephone calls to or from any similarly equipped vessel or shore station.

(d) Users can call a specific station, group of stations, or all stations to establish communication.

(2) DSC Distress Alert Receipt Policy. Units receiving DSC distress alerts shall first acknowledge receipt of the call via DSC and then attempt to establish voice communication on an appropriate channel. CC personnel shall 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.

(3) 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.

(4) General Digital Selective Calling (DSC) International Telecommunications Union (ITU) Requirements. The following policy applies:

(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 can be used;

(b) A station in the mobile or mobile-satellite service shall initiate and transmit a distress alert relay for a vessel that is unable to transmit a distress alert. The station transmitting the distress alert relay shall indicate it is not the vessel in distress; and

(c) Coast stations and appropriate coast earth stations that receive distress alerts shall route the alert as soon as possible to the RCC.

Note: Radiotelephone distress acknowledgement responsibilities can be found in Reference (x).

(5) 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[1]	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

[1] Very High Frequency-Frequency Modulation (VHF-FM) Channel 70 (156.525 MHz). This frequency is used in the maritime mobile service for digital selective calling, including DSC distress and safety calls. Use of this frequency for voice and communication other than DSC is prohibited.

b. Navigational Telex (NAVTEX). NAVTEX uses narrow-band direct-printing telegraphy for transmission of navigational and meteorological warnings and urgent information to ships on MF. NAVTEX is a service specifically designed for the promulgation of maritime safety information as a part of the GMDSS. All SOLAS-regulated ships are required to carry NAVTEX receivers. NAVTEX coverage 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.

   Note: See Chapter 11 of this Manual for further information regarding NAVTEX broadcasts.

c. Simplex Teletype Over Radio (SITOR). SITOR is a long-range service for use in ship-to-shore and shore-to-ship communication as part of the GMDSS for maritime safety information, and can be used as an alternative to satellite communication. SITOR employs a FEC mode of data for maritime safety broadcasts and ARQ for other transmissions to minimize the effects of poor HF propagation conditions.

   Note: See Chapter 11 of this Manual for further information regarding SITOR broadcasts.

d. Inmarsat. Virtually all navigable waters (less Polar Regions) of the world are covered by Inmarsat satellites. Inmarsat terminals provide telephone, data, facsimile, TELEX, email, and videoconferencing capabilities. Inmarsat provides service access codes for medical advice and medical assistance. The following section describes the three basic types of current 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. Used for distress alerting, data communication, and reception of maritime safety information. The Inmarsat C system offers two way data communication. Some terminals have message preparation capabilities while others have ports to connect to a personal computer. TELEX, email, and distress messages similar to an EPIRB alert message can be sent from this type of terminal. Additional information on the Inmarsat C is in the following section.

(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 maritime safety information 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. In addition,

[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, and

[3] SafetyNET service is provided through the satellite provider's web interface, and via voice operator in case of internet failure, per Reference (c). 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.

e. Radiotelephone. Radiotelephone is telecommunication by voice radio. CG radiotelephone operators must be well trained and proficient and, as CG representatives, shall always be professional. Military radiotelephone procedures shall be per Communication Instructions Radio Telephone Procedures, ACP 125 (series). All other radiotelephone procedures shall be per Reference (x) and ITU Regulations. Area and district commanders, commanders of logistics commands, and unit commanding officers shall ensure all operational shore units under their control follow the procedures per the Communications Watchstander Qualification Guide, COMDTINST M16120.7 (series) for preparing personnel for duties as communication watchstanders. The following is a list of common radiotelephone frequencies used by the CG for SAR communications (CG shore unit, vessel, and aircraft minimum guard requirements are in Chapters 7, 8, and 9 of this Manual):

(1) Medium Frequency (MF) Radiotelephony.

(a) 2182 kHz. International calling and distress frequency for radiotelephony. This frequency is used by ships and can be used by aircraft stations in an emergency. Shipping traffic in the vicinity of the DSC distress caller may not be able to receive this traffic. ITU Regulations dismisses the three minute silence period observed at the top and bottom of the hour on this frequency.

(b) 2670 kHz. Working frequency between CG stations and stations of the maritime community after initial contact is established on 2182 kHz.

(2) 4125 Kilohertz (kHz) High Frequency (HF) Radiotelephony. GMDSS voice frequency that has a dual role within the D17 AOR as a distress and hailing voice frequency.

(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.

(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 (156.800 MHz). VHF-FM Channel 9 (156.45 MHz) can be used by

recreational vessels for general purpose calling. This frequency shall be used whenever possible to relieve congestion on VHF-FM Channel 16 (156.800 MHz). Safety and distress broadcasts shall continue to be announced on VHF-FM Channel 16 (156.800 MHz).

(c) Very High Frequency – Frequency Modulated (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).

(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. 123.1 MHz is the aeronautical auxiliary frequency used by stations of the aeronautical mobile service and by other mobile and land stations engaged in coordinated search and rescue operations.

(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. Aircraft and survival craft can 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 appropriate authorities and completed in the first 5 minutes of each hour.

f. Satellite EPIRB. Used for distress alerting and locating survivors of distress incidents (406 MHz). 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 emergency locator transmitter (ELT) but national regulation can 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 FAA regulations. Personal locator beacons (PLB) 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, shall perform any and all acts necessary to rescue and aid persons and protect and save property. The procedures for terminating EPIRB signals can be found in Reference (a).

g. 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 this Chapter can be used in lieu of the SART. The following section provides further information on 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 shall be at least 96 hours.

h. Automatic Identification System-Search and Rescue Transmitter (AIS SART). This is a SAR transmitter used for locating survival craft. The AIS SART can 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). The following section provides further information on the AIS SART.

(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 shall be at least 96 hours.

F. 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, 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) shall assign and manage CG MMSIs. Newly established CG shore and afloat units without an MMSI can request one from Commandant (CG-652). Acquisition activities shall coordinate with Commandant (CG-652) to obtain a MMSI for new equipment. For replacement equipment, the MMSI would be transferred to the replacement equipment as it is installed by the regional base C4IT division/ESD or other installing activity.

3. Maritime Mobile Service Identity (MMSI) Search and Rescue (SAR) Vessel Identification System. The MMSI Vessel Identification System is a web-based

application managed by OSC, Martinsburg: http://misle.osc.uscg.mil/mmsi/. New user guidance can be found at: http://mislenet.osc.uscg.mil/.

G. False Alert Violation Reporting Policy. See Chapter 6 of this Manual.

CHAPTER 13 COAST GUARD (CG) RECORD MESSAGING, EMAIL, CHAT, AND TEXT MESSAGING

A. General. The policies in this Chapter apply to record messaging, email, chat services, Microsoft Office Communicator, and text messaging. Record message originators shall determine if the information in the record message can be passed quickly and efficiently via other means (e.g., secure telephone, email, SIPRNET chat, operational voice circuits); thereby, eliminating the need for the record message. For all procedural matters, see Reference (a).

B. Record Messaging. Record messages are the primary method by which the CG and other government agencies exchange official communications between commands.

1. Coast Guard (CG) Record Messaging System (CGRMS). CGRMS is comprised of several subsystems for processing both classified and unclassified record message traffic. CGRMS provides routing to various CG, DOD, and allied commands, along with other federal agencies. CG and DOD record messaging capabilities are described in the following section.

a. Coast Guard Record Messaging Capabilities. The following section describes CG record messaging capabilities.

(1) Shore based Unclassified CG Message System (CGMS) is available via CGOne for processing SBU and below record messages.

(2) Shore based Classified CG Message System (C-CGMS) is available via the SIPRNET system for processing classified (secret and below) record messages.

(3) Shore based TS collateral and SCI messaging service is provided through the Office of Naval Intelligence Hopper Information Service Center. The multi-media message manager application is used to view, draft and release TS collateral/SCI information. SCI message format/procedures are governed by Defense Intelligence Agency Operating Instruction (DOI) 103, Defense Special Security Communications System (DSSCS) Operating Instructions System/Data Procedures.

(4) Afloat message capabilities are comprised of multiple CG or Navy solutions that vary by platform. With a few exceptions, CGMS is the primary message drafting tool for Top Secret classification and below record messages. The primary SCI message drafting tool is the Navy SCI message editor, which is platform/equipment specific. For additional information regarding specific afloat message systems, contact the area CAT.

b. Department of Defense (DOD) Record Messaging Capabilities. The following section describes DOD record messaging capabilities used by the CG.

(1) Defense Message System (DMS) and Automated Message Handling System (AMHS). DMS/AMHS is an organizational messaging system developed by the DOD based on commercially available software. There are multiple DOD-wide record messaging systems; all interconnect with or utilize the DMS architecture.

(2) 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.

Note: Further information on CGRMS is located on the CG portal at: https://cgportal2.uscg.mil/units/tiscom/SitePages/Messaging%20Systems.aspx.

2. Inviolability of Record Messages. Distribution of record messages and the location of record message files shall prevent unauthorized viewing or access. At a minimum, 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 email or FAX to non-addressees simply for ease of providing others the same information. Record messages that are not received via the CGRMS shall not be considered official record; and

e. Internet releasable information via official CG record message.

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 shall be 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.

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". Chapter 2 and Chapter 5 of this Manual contain further information on operational telecommunication policies and the unauthorized disclosure of information. The following section provides further information on the internet release of record messages.

   a. CAMSLANT is designated as the only authorized organization to post record messages to the internet. In addition,

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

      (2) Address non-general distribution record messages requiring public release to COGARD CAMSLANT CHESAPEAKE VA. Section B.7 of this Chapter defines general record messages; and

      (3) Once internet released information has been posted to the official website, individuals can 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) might not be current or accurate and shall not be used as a source of official CG information.

      Note: For additional direction on internet release of CG directives, refer to The Coast Guard Directives System, COMDTINST M5215.6 (series).

5. Record Message Classes. The three classes of government record messages handled by the record message system are:

   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; and

   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.

6. Emergency Command Precedence. The emergency command precedence (Y) is not authorized for CG use.

7. General Record Messages. General record messages are intended to meet recurring requirements for the dissemination of information to predetermined standard distribution. The following section provides further information on general record messages.

   a. Description. General record messages have specific titles used to determine the distribution. 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);

      (2) All CG officers (ALCGOFF);

      (3) All CG enlisted (ALCGENL);

      (4) All CG Personnel Service Center (ALCGPSC);

      (5) All CG reserve (ALCGRSV);

      (6) All CG civilian (ALCGCIV);

      (7) All CG finance (ALCGFINANCE); and

      (8) All CG recruiting (ALCGRECRUITING).

   b. General Record Message Originators. General record messages originating policy is provided in the following section.

      (1) Coast Guard (CG) Originators. The following policy applies:

         (a) ALCOASTS. Commandant, Vice Commandant, Headquarters Flag/Senior Executive Service (SES) positions, Force Readiness Commander, National Command Center, and the Master Chief Petty Officer of the CG concerning matters under their authority. These principles may delegate this authority by name to persons acting on their behalf. Such delegation shall be provided via memo to CAMSLANT and Commandant (CG-09EA); and

         (b) All Other CG General Messages. Commandant, area and district commanders, and Commander CG Personnel Service Center.

(2) United States Navy (USN) Originators. 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. General Record Message Cancellation. Record message cancellation is the responsibility of the originator. There are three methods used to cancel general record messages:

(1) For some general record message series, the first record message released in the calendar year is a recapitulation message. The recapitulation message designates which record messages for that series remain in effective. All general record messages of the series not listed in the recapitulation message are cancelled at the end of 1 year from the record message date-time-group. The following applies:

(a) This period of time can be extended by a subsequent general record message of the same series within 1 year of the original record message. The subsequent general record message shall state the date the record message is cancelled; and

(b) If one year has passed and no extension of time has been affected, a general record message must be reissued if it is to remain effective.

(2) Cancellation record messages can be sent at other times during the year; or

(3) An individual general record message can include its own cancellation date within the text.

d. General Record Message Review/Recapitulation. The following policy applies for the review and recapitulation of general record messages:

(1) Originators shall continuously review their posted information for applicability throughout the year and immediately advise the CAMSLANT of any outdated information; and

(2) Originators shall submit an annual recap of their effective general record messages to the CAMSLANT no later than 31 January of each calendar year.

e. General Messages on CG Portal. Units requiring CG, USN, and joint general record messages can find them at: https://cgportal2.uscg.mil/library/generalmessages/SitePages/Home.aspx.

Note: After 31 January of each calendar year, all general record messages older than one year but still effective are moved to the "Effective Messages" portion of the general message archive site on the CG Portal. Originators are still responsible to review the "Effective Messages" site and promptly advise CAMSLANT of any outdated information.

f. Applicability and Distribution. Headquarters units and area staffs shall coordinate with CAMSLANT to ensure routing guard lists for general messages remain accurate.

8. Plain Language Addresse (PLAs). PLAs are unit identifiers of a record message's command authority.

9. Collective Addresses. The term "collective address" refers to a CAD, AIG, or task organization (TASK). The following section outlines CAD, AIG, and TASK policy.

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. CADs shall be comprised of a minimum of 30 PLAs and must be used a minimum of 15 times per calendar year.

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. An AIG shall be comprised of a minimum of 30 PLAs, and must be used a minimum of 15 times per calendar year.

c. Task Organization (TASK). TASK groups shall be established and maintained by individual units.

d. CAD/AIG Recapitulation. The cognizant authority is the commander responsible for the composition and use of the CAD/AIG. The following guidelines apply:

(1) Cognizant authorities must recapitulate each CAD/AIG at least once per year or when 10 modifications have been issued;

(2) Cognizant authorities shall ensure each CAD/AIG maintains a minimum of 30 members;

(3) CAMSLANT's directory services manager is authorized to act in place of the cognizant authority for CG owned CAD/AIGs for the purpose of creation, modification, maintenance and disestablishment; and

(4) Cognizant authorities shall route any changes to CAD/AIGs through the directory services manager.

10. Staff Symbols. Staff symbols provide routing, processing, and filing guidelines for correspondence and record message systems. Staff symbols are required with headquarters, area, logistic centers, service centers and district PLAs. A list of authorized staff symbols for CG record messages is in Standard Distribution List, COMDTNOTE 5605 (series). Staff symbols are no longer required for record messages destined for USN commands.

11. Standard Subject Indicator Code (SSIC). An SSIC is not required for CG originated messages unless destined to an allied/NATO PLA, AIG, CAD or task organization. The Standard Subject Identification Codes (SSIC) Manual, COMDTINST M5210.5 (series) contains a complete list of SSICs for CG use.

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

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

    a. Originator Responsibilities. Commanding officers are ultimately responsible for assigning the appropriate precedence before releasing record messages and shall ensure the guideline for precedence assignment in Reference (a) are enforced.

    b. Addressee Responsibilities. The addressee responsibilities for meeting SOSOs are as follows:

        (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. Communication Area Master Station (CAMS) Responsibilities. To assist with meeting SOSO objectives, the CAMS shall:

        (1) Monitor record message systems for performance and backlogs; and

        (2) Assist units with record message delivery problems.

14. Tracer Action. A tracer action enables the CAMS 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 in Reference (a). The record message originator shall initiate tracer action for record messages reported as non-delivered.

15. High-Precedence Record Message System Testing. In order to determine record message system performance and unit notification capabilities, Areas shall conduct quarterly high-precedence record message system testing using the flash precedence only. Areas shall determine the high-precedence test results using the time the test record message populates the addressee's record message folders rather than the time-of-receipt of the test message record message response. In addition, the following applies:

    a. Areas shall test both 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.

    c. Areas shall track the following results of high-precedence tests:

        (1) Test record message DTG;

        (2) Addressees;

        (3) Addressees' operational status;

        (4) Times of record message folder delivery and time of notification that the record message was acknowledged by the addressees;

        (5) If applicable, reason SOSO was not met; and

        (6) Other problems encountered with the test.

16. Record Message Text. The text of a record message is defined as the section of the record message below the subject line. The following policy applies to record message text:

    a. Upper and lower case letters can be used for the text of CG generated record messages, except for the record messages listed in paragraph (b) of this section;

    b. PROFORMA (e.g., CASREP), general administrative (GENADMIN) formatted, and all record messages destined for automatic broadcast (e.g., NAVTEX) shall be drafted in upper case only; and

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

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

17. Other Record Message Actions. See Reference (a) for procedures on record message cancellations, corrections, acknowledgements, readdressals, and quoting, as well as, procedures for "canned" (PROFORMA) record messages.

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

1. Organizational Electronic Mail (Email). Organizational email is defined in Management of Electronic Mail, COMDTINST 5270.1 (series) as email between organizational elements that requires approval by officials with signature authority. Such correspondence must be released by command authority and shall 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." CGOne meets requirements for encryption of FOUO information. However, official CG email and record messages shall not be auto-forwarded outside the protected environment of CGOne.

2. Personal Use of Email. Specific guidance on the personal use of email can be found in Reference (k).

D. 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 email, anyone with access to the chat room (which can be restricted to specific participants) can follow the thread as far back as necessary without having to be an addressee. The following policy applies:

1. Microsoft Office Communicator on CGOne is protected up to the level of UNCLAS FOUO/SBU information. For more information on the use of this application see Reference (j);

2. 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; and

3. 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. In addition,

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

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

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

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

2. When directed by Annex K to Area OPLAN, OPTASK, or SOP, significant text communications shall be recorded (manually if necessary) and saved as a communications log per Chapter 6 of this Manual.

APPENDIX A GLOSSARY OF ACRONYMS AND TERMS

--- (A) ---

AA	Advice and assist
ACP	Allied Communications Publication
ADCON	Administrative control
AES	Advanced Encryption Standard
AIG	Address indicating group
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
ALCGENL	All Coast Guard enlisted
ALCGFINANCE	All Coast Guard finance
ALCGOFF	All Coast Guard officer
ALCGPSC	All Coast Guard Personnel Service Center
ALCGRECRUITING	All Coast Guard recruiting
ALCGRSV	All Coast Guard reserve
ALCOAST	All Coast Guard
ALE	Automatic link establishment
ALTERS	Allied Telecommunications Record System
AMHS	Automated Message Handling System
ANI	Automated number identification
AOR	Area of responsibility
ATA	Automatic test call answering
ARQ	Automatic repeat request
AUTODIN	Automatic Digital Network

--- (B) ---

BNM	Broadcast Notice to Mariners
BRI	Basic Rate Interface

--- (C) ---

C3CEN	Command, Control, and Communications Engineering Center
C4	Command, control, communication, and computers
C4I	Command, control, communication, computers, and intelligence
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
C4IT SC	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
CC	Command center
C-CGMS	Classified Coast Guard Message System
CCI	Cryptographically controlled item
CCP	Contingency Communications Plan
CE	Categorical Exclusion
CEP	Continuous evaluation program
C.F.R	Code of Federal Regulations
CG	Coast Guard
CGMS	Coast Guard Message System
CGOne	Coast Guard One Network
CGRMS	Coast Guard Record Messaging System
CGTS	Coast Guard Telecommunication System
CIC	Combat information center
CIL	Critical information list
CIRM	International Radio Medical Center
CJCS	Chairman, Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CLUAS	Card Loader User Application Software
CMC	Classified material control
CMCS	COMSEC Material Control System
CMS	COMSEC Material System
CMWS	COMSEC management workstation
CNO	Chief of Naval Operations
COCOM	Combatant commands
COLNAV	Columbian Navy
COMDTINST	Commandant Instruction
COMMSHIFT	Communication guard shift
COMMSTA	Communication station
COMMSYS	Communication System
COMNAVSECGRU	Commander, Naval Security Group Command
COMNETWARCOM	Commander, Naval Network Warfare Command

COMSATCOM	Commercial satellite communication
COMSEC	Communication security
COMSPOT	Communication spot
COMTAC	Communications tactical
COOP	Continuity of operations
COR	Contracting officers representative
COSPAS-SARSAT	Cosmicheskaya Sistyema Poiska Avariynich Sudov - Search and Rescue Satellite-Aided Tracking
COTHEN	Cellular over the Horizon Enforcement Network
CRF	Crypto Repair Facility
CSN	Communication Systems Network
CUAS	Common User Application Software
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
DH	Deadhead (no charge)
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DMD-PS	Data management device – power station
DMS	Defense Messaging System
DNI	Director of National Intelligence
DOD	Department of Defense
DOI	Defense Intelligence Agency Operating Instruction
DON	Department of Navy
DPRI	Directives, Publications and Reports Index
DRS	Disaster Recovery System
DSC	Digital selective calling
DSL	Digital subscriber line
DSN	Defense Switch Network
DSSCS	Defense Special Security Communications System
DTG	Date-time group
DVL	Digital voice logger

--- (E) ---

EAIS	Encrypted Automatic Identification System

ECU	End crypto equipment units
EEFI	Essential elements of friendly information
EGC	Enhanced group call
EHF	Extremely high frequency
EMSS	Enhanced Mobile Satellite Service
EKMS	Electronic Key Management System
ELMR	Enterprise land mobile radio
ELT	Emergency locator transmitter
Email	Electronic mail
EMCON	Emission control
EMSEC	Emission security
EO	Executive Order
EPIRB	Emergency position-indicating radio beacon
ESD	Electronic Systems Support Detachment
ESU	Electronic Systems Support Unit

--- (F) ---

FAA	Federal Aviation Administration
FAX	Facsimile
FCC	Federal Communications Commission
FEC	Forward error correction
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FORCECOM	Commander, Forces Training Command
FOUO	For official use only
FRC	Federal Records Center
FSS	Fixed Satellite Service
FTS	Federal Telephone Service
FWTS	Federal Wireless Telecommunications Services

--- (G) ---

GENADMIN	General administrative
GETS	Government Emergency Telecommunications Service
GMDSS	Global Maritime Distress and Safety System
GOTHAM	Geo-Spatial over the Horizon ALE Matrix
GPS	Global Positioning System
GSA	General Services Administration
GSM-SM	Global system for mobile communication security module

--- (H) ---

HF	High frequency
HF-ALE	High frequency-automatic link establishment

HIPAA	Health Insurance Portability and Accountability Act
HLS Net	Homeland Security Network

--- (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
ID	Identification
ID3	International direct distance dialing
IEC	International Electrotechnical Commission
IMEI	International Mobile Equipment Identity
IMH	Incident Management Handbook
IMO	International Maritime Organization
IMPAC	International merchant purchase authorization card
INFOSEC	Information security
INTERCO	International Code of Signals
IP	Internet protocol
IRR	International Radio Regulations
ISDN	Integrated Services Digital Network
ISIC	Immediate-superior-in-command
ISM	Iridium security module
ITOC	IT Operations Center
ITU	International Telecommunications Union
IW	integrated waveform
IWN	Integrated Wireless Network

--- (J) ---

JANAP	Joint Army, Navy, Air Force Publication
JIACC	Joint Inter-agency Counterdrug COMSEC
JIATF	Joint Interagency Task Force
JIST	Joint Integrated Satellite Communications Tool
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
kHz	Kilohertz

KMF	Key Management Facility
KP	Key Processor
KVL	Key variable loader
	--- (L) ---
LANTAREA	Atlantic area
LANTCOMMSYS	Atlantic Area Communication System
LCMS	Local COMSEC Management Software
LE	Local Element
LE(I)	Local Element (Issuing)
LEC	Local exchange carrier
LE Sensitive	Law enforcement sensitive
LMD	Local Management Device
LOA	Letter of Agreement
LPD	Low probability of detection
LPI	Low probability of intercept
LPID	Low probability of identification
	--- (M) ---
MCC	Mobile command center
MDT	Message distribution terminal
MEDICO	Medical communications
MF	Medium frequency
MHz	Megahertz
MILSATCOM	Military satellite communication
MISLE	Marine Information for Safety and Law Enforcement
MMSI	Maritime mobile service identity
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multi-protocol label switching
MSS	Mobile Satellite Service
MUOS	Mobile User Objective System
	--- (N) ---
NAFA	Non-appropriated funds activity
NAIS	Nationwide Automatic Identification System
NATO	North Atlantic Treaty Organization
NAVAREA	Navigational area
NAVCEN	Coast Guard Navigation Center
NAVTEX	Navigational Telex
NCA	National Command Authority
NCMS	Naval Communication Security Material System
NCS	National Communications System

NCTAMS	Naval Computer and Telecommunications Area Master Station
NDRS	National Distress and Response System
NECN	National Emergency Communications Network
NECOS	Net control station
NGA	National Geospatial-Intelligence Agency
NIMS	National Incident Management System
NIPRNET	Non-classified internet protocol router network
NIST	National Institute of Standards and Technology
NLECC	National Law Enforcement Communications Center
NOAA	National Oceanic and Atmospheric Administration
NOFORN	Not releasable to foreign nationals
NORTHCOM	United States Northern Command
NSA	National Security Agency
NS/EP	National security and emergency preparedness
NSI	National security information
NSS	National Search and Rescue Supplement
NSPD	National Security Systems Policy Directive
NTIA	National Telecommunications and Information Administration
NTISSD	National Telecommunications and Information Systems Security Directive
NTP	Naval Telecommunications Procedures
NWP	Naval Warfare Publications
NWS	National Weather Service

--- (O) ---

OINC	Officer in Command
OMB	Office of Management and Budget
OPCON	Operational control
OPLAN	Operations plan
OPNAVINST	Office of the Chief of Naval Operations Instructions
OPORDER	Operational order
OPSEC	Operations security
OPTASK	Operational tasking
OS	Operations specialist
OSC	Coast Guard Operations System Center
OSHA	Occupational Safety and Health Act
OTAR	Over the air rekeying

--- (P) ---

PACAREA	Pacific area
PACCOMMSYS	Pacific Area Communication System
PBX	Private branch exchange

PCII	Protected critical infrastructure information
PERSEC	Personnel security
PII	Personal identifiable information
PIN	Personal identification number
PLA	Plain language address
PRI	Primary Rate Interface
PROFORMA	Pre-formatted

--- (R) ---

R21	Rescue 21
RADIOFAX	Radio facsimile
RADLOGS	Radio logs
RASKL	Really simple key loader
RCC	Rescue coordination center
RFF	Remote fixed facility
RPC	Regional Planning Committee

--- (S) ---

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
SDLC	System development life cycle
SECDEF	Secretary of Defense
SECDHS	Secretary, Department of Homeland Security
SECNAV	Secretary of Navy
SES	Senior Executive Service
SHARES	Shared resources
SHD	Special handling designator
SILC	Shore Infrastructure Logistics Center
SIM	Subscriber identity module
SIPRNET	Secret internet protocol router network
SITOR	Simplex teletype over radio
SMC	SAR mission coordinator
SMEF	System Management and Engineering Facility
SMIB	Safety Marine Information Broadcast
SOLAS	Safety of life at sea
SOP	Standard operating procedure
SOSO	Speed of service objective

SPII	Sensitive personal identifiable information
SSIC	Standard subject indicator code
STE	Secure telephone equipment
	--- (T) ---
TACON	Tactical control
TACT	Tailored annual cutter training
TASK	Task organization
TBA	Terminal base address
TCO	Telecommunications Certification Office
TCP/IP	Transmission control protocol/internet protocol
TCTO	Time compliance technical order
TIN	Tactical Information Network
TISCOM	Telecommunication and Information Systems Command
TRANSEC	Transmission security
TS	Top Secret
TSP	Telecommunication Service Priority
TSTA	Tailored ships training availability
TTP	Tactics, techniques and procedures
	--- (U) ---
UC	Unified communications
UFO	UHF follow-on
UHF	Ultra high frequency
UHF-FM	Ultra high frequency – frequency modulated
UMIB	Urgent marine information broadcast
UNCLOG	U.S. Coast Guard / National Weather Service Coordination-Liaison Working Group
UPS	Uninterruptible power supply
U.S.C.	United States Code
USN	United States Navy
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
VTC	Video teleconferencing
VTS	Vessel Traffic Service

--- (W) ---

WAN	Wide area network
WITS	Washington Interagency Telecommunications System
WPS	Wireless priority service

Index