



Commandant  
United States Coast Guard

2100 2nd St SW STOP 7101  
Washington, DC 20593-7101  
Staff Symbol: CG-652  
Phone: (202) 475-3542

COMDTINST 2000.4B

MAY 03, 2013

COMMANDANT INSTRUCTION 2000.4B

Subj: TELECOMMUNICATIONS STRATEGY (TCS)

Ref: (a) Telecommunication Manual, COMDTINST M2000.3 (series)

1. PURPOSE. This Instruction provides a strategy for evolution of the Coast Guard Telecommunication System (CGTS) to improve, integrate, and maximize telecommunications capabilities in support of mission execution. It also provides authority and guidance as a basis for Coast Guard telecommunications decisions on investments, policies and procedures, and operation.
2. ACTION. Area and district commanders, unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants and chiefs of headquarters staff elements shall ensure compliance with this instruction. Internet release is authorized.
3. DIRECTIVES AFFECTED. Telecommunications Plan (TCP), COMDTINST M2000.4A is canceled.
4. MAJOR CHANGES. None.
5. REQUEST FOR CHANGES. Submit recommended changes to Commandant (CG-65).
6. BACKGROUND. The Command, Control, Communications, Computers and Information Technology (C4&IT) Strategic Plan, published by the Assistant Commandant for C4&IT (CG-6), provides a unifying strategy for Commandant (CG-6) to improve, integrate, and maximize the Coast Guard's C4&IT capabilities in support of mission execution. It also aligns C4&IT goals to federal, Department of Homeland Security, and Coast Guard guidance. The TCS complements and works in conjunction with the C4&IT Strategic Plan by outlining authorities, strategies, goals and objectives specific to the Coast Guard Telecommunications Program. This was formerly accomplished via the Telecommunications Plan, a document that predates Commandant (CG-6).

DISTRIBUTION – SDL No. 162

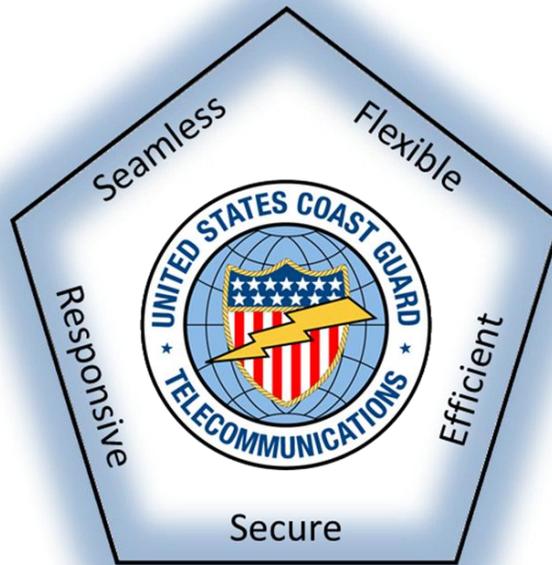
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	X	X	X	X	X	X			X	X	X		X	X								X				
B	X	X	X	X							X	X	X	X	X	X		X			X	X			X	
C	X	X		X	X			X	X							X	X								X	
D				X																X					X	
E																										
F																										
G			X	X	X																					
H						X	X																			

NON-STANDARD DISTRIBUTION:

7. POLICY. The TCS provides goals and objectives to define means to achieve a desired future state for the CGTS. All CGTS updates, improvements, modernizations, and consolidations shall be linked to this strategy and shall support valid telecommunications requirements. The TCS applies to all Coast Guard units.
8. PROCEDURES.
  - a. Requirements Identification and Validation. Telecommunication requirements generally originate from field commanders. The Office of C4 and Sensor Capabilities, Commandant (CG-761), evaluates and validates requirements. Planning and budgeting is prerequisite to implementation. Identification of solutions and implementation is under the purview of Commandant (CG-6), consistent with overarching strategies. The process for requirements identification and submission is outlined in reference (a).
  - b. TCS Maintenance. The TCS will be reviewed at least annually and revised as needed to reflect significant changes in requirements and new Coast Guard initiatives as well as changes in overall C4&IT or Telecommunications Program direction.
9. DISCLAIMER. This document is intended to provide operational requirements for Coast Guard personnel and is not intended to nor does it impose legally-binding requirements on any party outside the Coast Guard.
10. RECORDS MANANGEMENT CONSIDERATIONS. This Instruction has been thoroughly reviewed during the directives clearance process, and it has been determined there are no further records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., NARA requirements, and Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does not create significant or substantial change to existing records management requirements.
11. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental considerations under the National Environmental Policy Act (NEPA) were examined in the development of this Commandant Instruction. It is categorically excluded from further NEPA analysis and document requirements under Categorical Exclusion #33 as published in NEPA Implementing Procedures and Policy for Considering Environmental Impacts, COMDTINST M16475.1 (series), Figure 2-1. An Environmental Checklist and a Categorical Exclusion Determination (CED) are not required.
12. FORMS /REPORTS. None.

ROBERT E. DAY /s/  
Rear Admiral, U. S. Coast Guard  
Chief Information Officer

Encl: (1) Telecommunications Strategy (TCS) 2013 - 2017



# **U.S. Coast Guard Telecommunications Strategy (TCS) 2013 – 2017**

---

**Evolving NetCentric Telecommunications:  
A Strategy for Sustained Success**

## **1. Purpose.**

The Telecommunications Strategy (TCS) clearly defines the mission and establishes a vision for the future state of the Coast Guard's Telecommunication System (CGTS). Imparting obtainable goals and SMART<sup>1</sup> objectives, the strategy provides the direction and focus necessary for the capital investment in planning, development, and deployment, as well as investment control while ensuring mission sustainment.

## **2. Background.**

### **2.1. Coast Guard Telecommunication System (CGTS).**

The CGTS is a *system of systems* linking assets (shore units, aircraft, cutters, boats, and individual responders) to other agencies and organizations throughout the nation and world. The CGTS includes the transport mechanisms used to convey data and voice using network, radio, satellite, and telephone facilities that are owned/leased, controlled and/or used by the CG. This includes associated terminal facilities, equipment, and tools, along with associated policy, tactics, techniques, and procedures (TTP).

### **2.2. CGTS Operations.**

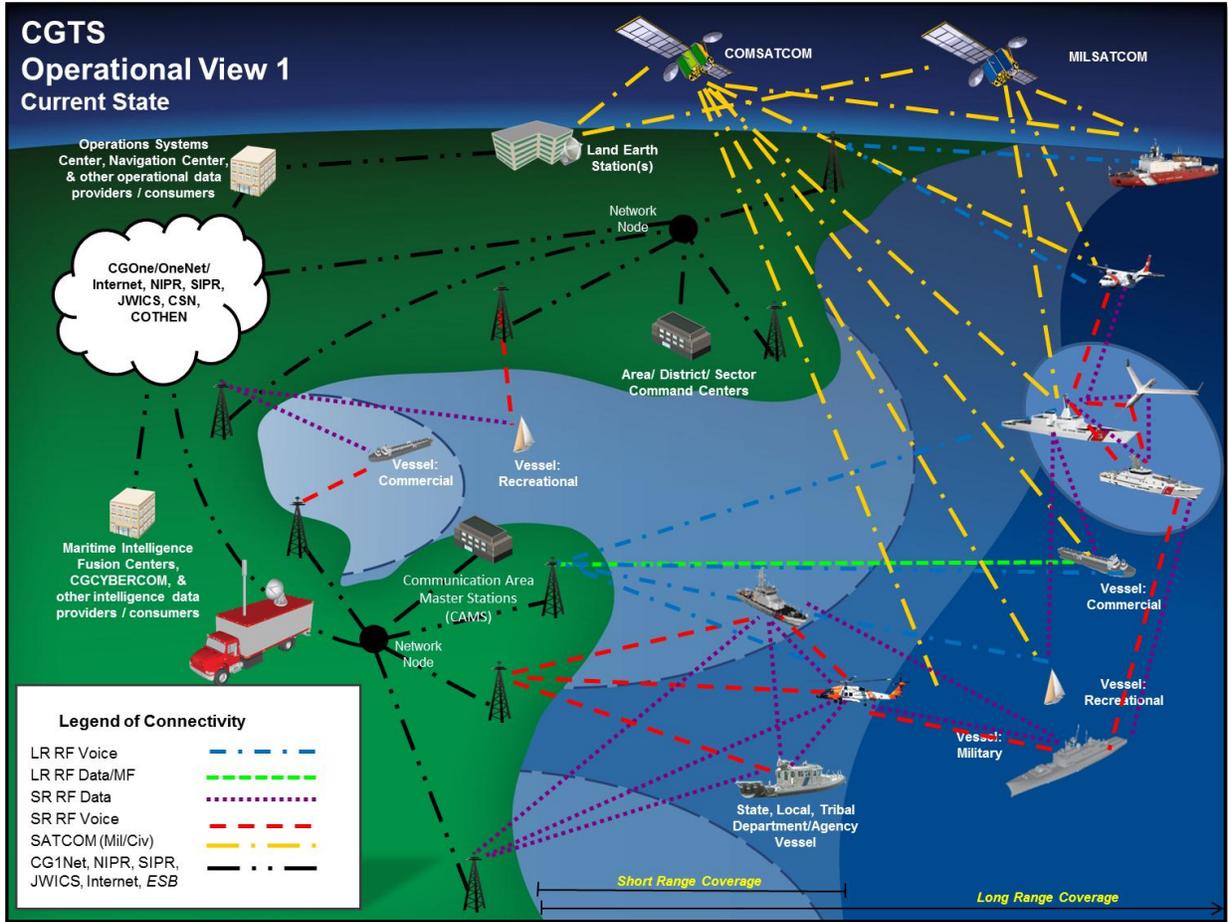
CGTS is governed by a substantial body of federal laws, regulations, international treaty obligations, internal policies and interagency agreements (see Appendix A). CGTS is operated by the Deputy Commandant for Mission Support (DCMS) through the Assistant Commandant for C4&IT (CG-6). It helps enable and supports CG mission execution as directed by the Deputy Commandant for Operations (DCO).

### **2.3. Operational View.**

Today's CGTS consists of a number of complex sub-systems supporting both operational command and control and intelligence (C2I), mission support, and administrative communications for personnel executing and planning every CG mission. Some of the major components include CGOne, Internet, Secret Internet Protocol Router Network (SIPRNet), Joint Worldwide Intelligence Communications System (JWICS), Rescue 21, the Long Range Communication System (COMMSYS) consisting of CAMS and COMMSTAs, commercial and military satellite systems, individual unit telephone systems, wireless systems, and mobile command centers. Figure 1 illustrates some of the many discrete systems comprising the CGTS.

---

<sup>1</sup> SMART – Specific, Measurable, Attainable, Relevant, Time-bound



**Figure 1 - CGTS Current Operational View  
Dissimilar Telecommunication Services**

### 3. Telecommunications Strategy.

#### 3.1. Mission Statement.

The Mission of CGTS is to:

- a. Provide and maintain rapid, reliable, secure, 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.

### 3.2. Vision Statement.

CGTS is a fully integrated and seamless NetCentric telecommunications architecture delivering secure, efficient, responsive, and flexible operational communications worldwide.

- Communications Working Group, June 2012

### 3.3. Future State of CGTS.

Figure 2 shows a future end state where data and information flow seamlessly over CGTS, reaching intended recipients regardless of transmission medium.

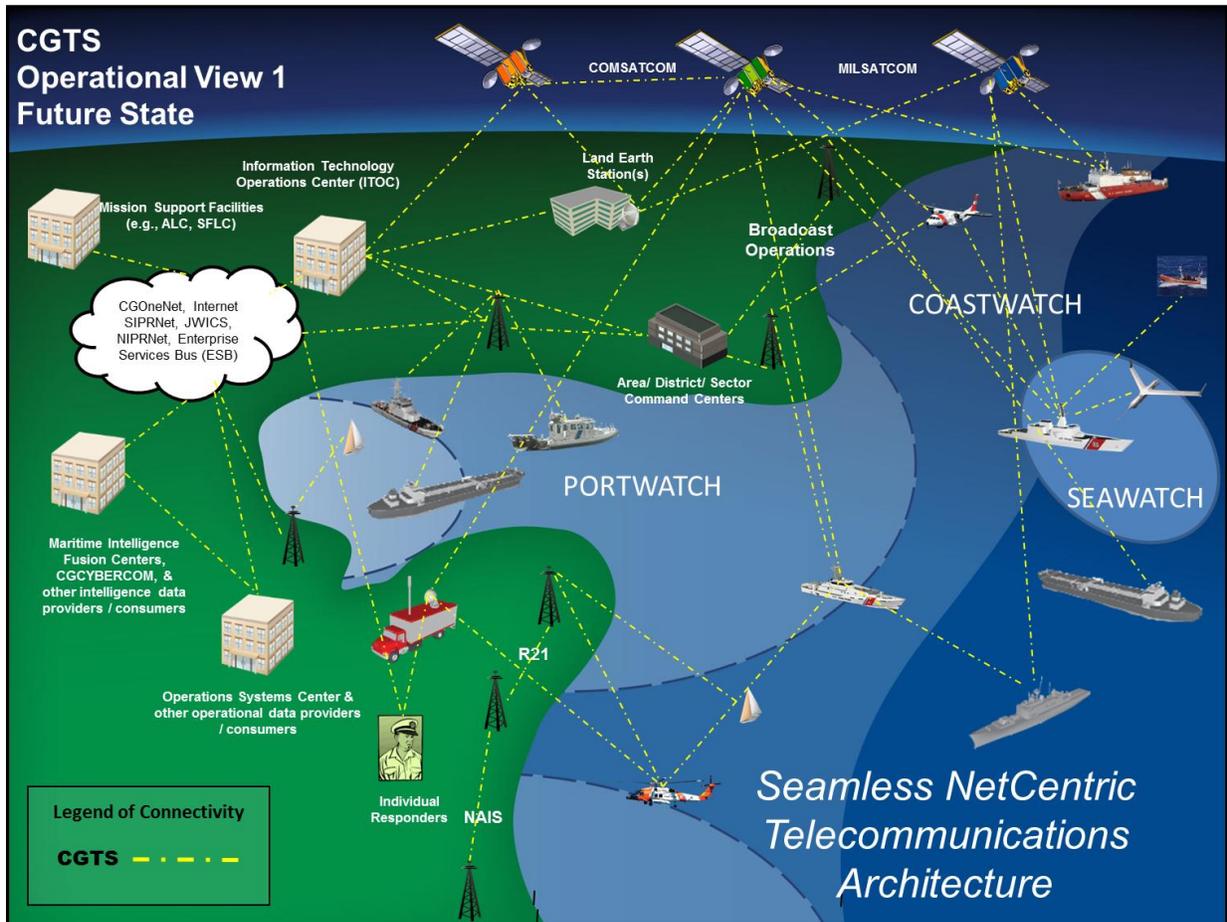


Figure 2 - CGTS – Future State Operational View of Seamless Telecommunication Services

### **3.4. Discussion.**

CGTS has steadily evolved over the years within the continuum of technological advancement. Analog networks and individual stove piped systems are being replaced by high speed digital networks, open computing environments, digital wireless and video devices, and software driven radios, all based on commercial-off-the-shelf (COTS) solutions. Ultimately, this evolution can deliver a seamless telecommunications environment where digital information, be it audio, video or data, is delivered when and where necessary, regardless of transmission means.

As it evolves into the envisioned NetCentric state, CGTS must continue to provide the services the Coast Guard, its customers, and partners depend upon for successful mission prosecution and the safety of life at sea. Otherwise stated, an effective strategy must ensure the successful integration of discrete communication systems, provide the means by which to address mission needs, and simultaneously sustain services and implement operational constructs with both mission and customer needs in mind. Thus, the strategy provides not only a future vision and end state to guide investments, but also establishes a foundation for success.

The concept of NetCentric Communications coupled with a NetCentric Telecommunications Architecture form the basis for the vision of the future CGTS.

#### **3.4.1. NetCentric Communications.**

NetCentric Communications is the concept of a continuously evolving, complex community of people, devices, information and services interconnected by communications networks to achieve optimal benefit from limited resources through better coordination of events and their consequences. In military connotation, it is frequently associated with terms "NetCentric Operations (NCO)" and "NetCentric Warfare (NCW)" wherein NetCentric refers to activities that cross multiple networks.

#### **3.4.2. NetCentric Telecommunications Architecture.**

A NetCentric Telecommunications Architecture is defined as a massively distributed architecture with components and/or services available across and throughout an enterprise's entire lines-of-business. As the architecture evolves, various information transport capabilities converge along with associated information sources and applications into a more seamless and less labor intensive environment.

### **3.5. Strategic Goals and Objectives.**

Derived directly from the Vision Statement, five strategic goals form the foundation of the strategy. This foundation, when coupled with the objectives, provides the Coast Guard with an efficiently managed, adaptive telecommunication environment, capable of sustained technological evolution through continual integration of communication systems as they mature throughout the 21st century.

**Goal 1 - Fully integrate systems to operate across a seamless NetCentric Telecommunications Architecture**

**Goal 2 – Ensure a secure operating environment**

**Goal 3 – Operate efficiently**

**Goal 4 – Provide operationally responsive services**

**Goal 5 – Deliver flexible services**

#### **Goal 1 – Fully integrate systems to operate across a seamless NetCentric Telecommunications Architecture**

This goal articulates the desired end state for CGTS wherein dissemination of information is unconstrained by any given transport system.

##### **Objective 1.1 - Open architecture with standards-based implementation**

Embrace National/Regional/International industry standards that provide an interoperable non-proprietary environment. A standards-based architecture permits implementation of a wide variety of COTS solutions such as voice over IP (VOIP) telephony and conversion of radio frequency (RF) networks to IP based networks with software driven radios. This provides the desired seamless transport mechanism for system integration and evolution. This objective is measured against the full implementation of Enterprise Architecture standards and the successful integration of individual fielded systems to provide networked services.

##### **Objective 1.2 - ESB transport service provider**

Establish the CGTS as the transport service provider for the Enterprise Services Bus (ESB). ESB subscription services will be obtained through the CGTS. This objective is measured as the percentage ESB services transported by CGTS.

##### **Objective 1.3 – Communications Common Operational Picture (CCOP)**

Establish fully integrated CCOP overlay of the operational communications environment. This is measured against the automated reporting of individual systems into the CCOP and its usefulness/timeliness in meeting the requirements of the operational commander.

**Goal 2 – Ensure a secure operating environment**

This goal places focus on assurance and sustainment of services.

**Objective 2.1 - Inviolable services**

Instill and sustain quality assurance processes such that users trust the CGTS to deliver the right information where and when necessary. This is measured against CGTS availability, and sustained confidentiality.

**Objective 2.2 – Information Technology Operations Center (ITOC) providing proactive cyber defense in depth across domains**

Expand the ITOC into a hardened facility capable of acting on behalf of the entire enterprise, individual units, and deployed assets to mitigate outages and cyber threats. Coordinate ITOC operations in step with Department of Defense (DOD) cyber initiatives and provide sufficient capability to assure information delivery in an increasingly hostile network environment. This is measured as sustained operations against threats.

**Objective 2.3 - High speed cross domain transport**

Reduce the time and complexity of transferring information between varying levels of classified, protected, and unclassified networks, expanding current capabilities to the .mil/smil.mil security domains. This is to be measured against the current operational baseline.

**Goal 3 – Operate efficiently**

This goal expresses the need to provide the best possible services against the realities of budgetary, operational, and technical constraints.

**Objective 3.1 - Best possible Return on Investment (ROI)**

Field technologies that meet operational requirements and provide fair value to the nation's tax payers. This objective is measured against the calculation of actual ROI against the planned ROI of fielded systems as defined within SDLC documentation and against the execution of agency budget (AFC-36, AFC-42).

**Objective 3.2 - Optimally managed**

Leverage technology to provide the best possible systems while considering efficient administration of CGTS services to achieve the best possible balance between effectiveness and efficiency. This effectiveness is measured as the ratio of operational availability to total cost of ownership.

#### **Goal 4 – Provide operationally responsive services**

This goal places focus on organizational responsibilities for CGTS operations.

##### **Objective 4.1 - Governance compliant**

Ensure CGTS complies with the regulatory environment to include laws, treaties, federal regulations, departmental and agency instructions, and other approved service level agreements. This includes the promulgation and implementation of effective telecommunications policy to meet the objectives and goals of DHS and the Coast Guard CIO. This is measured against the requirements for compliance established within all relevant documents, a list of the more important of which are included as Appendix A.

##### **Objective 4.2 – Resiliency with sustainable contingency response**

Employ the most efficient means to sustain, surge, and/or rapidly restore services in the event of emergent mission requirements, services degradation or failure. This is measured against stated requirements for individual systems, and/or service level agreements, operational impact of failure, and the capabilities of deployable contingency response forces and equipment to meet mission requirements.

##### **Objective 4.3 – Alternative routing of critical information**

Establish multiple paths to pass mission critical C2I information on behalf of the operational commander. Identify and map mission critical information elements, develop alternative routing methodologies, and implement exercise regimens for secondary and tertiary (if deemed necessary) communication paths. Examples include blue force tracking, status reporting, field intelligence reporting and chat/text messaging capabilities in a bandwidth constrained environment. This is measured against the ability of secondary (or tertiary) paths to effectively deliver mission critical information to the intended recipient within prescribed timeframes.

##### **Objective 4.4 - Faster technology infusion**

Reduce the time to field new systems given acquisition regulatory constraints and the need to ensure internal process compliance. This includes proactive outreach to our personnel and our partners to fully understand and internalize their requirements. This is measured against planned vs. actual achieved goals established in individual project plans and time required for internal processing of documentation to effect changes (e.g., technologies refresh processes).

**Goal 5 – Deliver flexible services**

This goal incorporates operational requirements to provide varying levels of services on demand.

**Objective 5.1 – Platform independence**

Provide network services to all assets requiring the service. In other words, a user may be afloat, aloft or ashore and still able to sustain access to networked services within the constraints of the operating environment. This objective is measured against the successful provision of the best possible services available to specific fielded platforms (aircraft, ships, boats, shore units, and individual responders) within physical, technical and financial constraints.

**Objective 5.2 - Fully interoperable with DOD while sustaining DHS, OGA and civilian maritime community interoperability requirements**

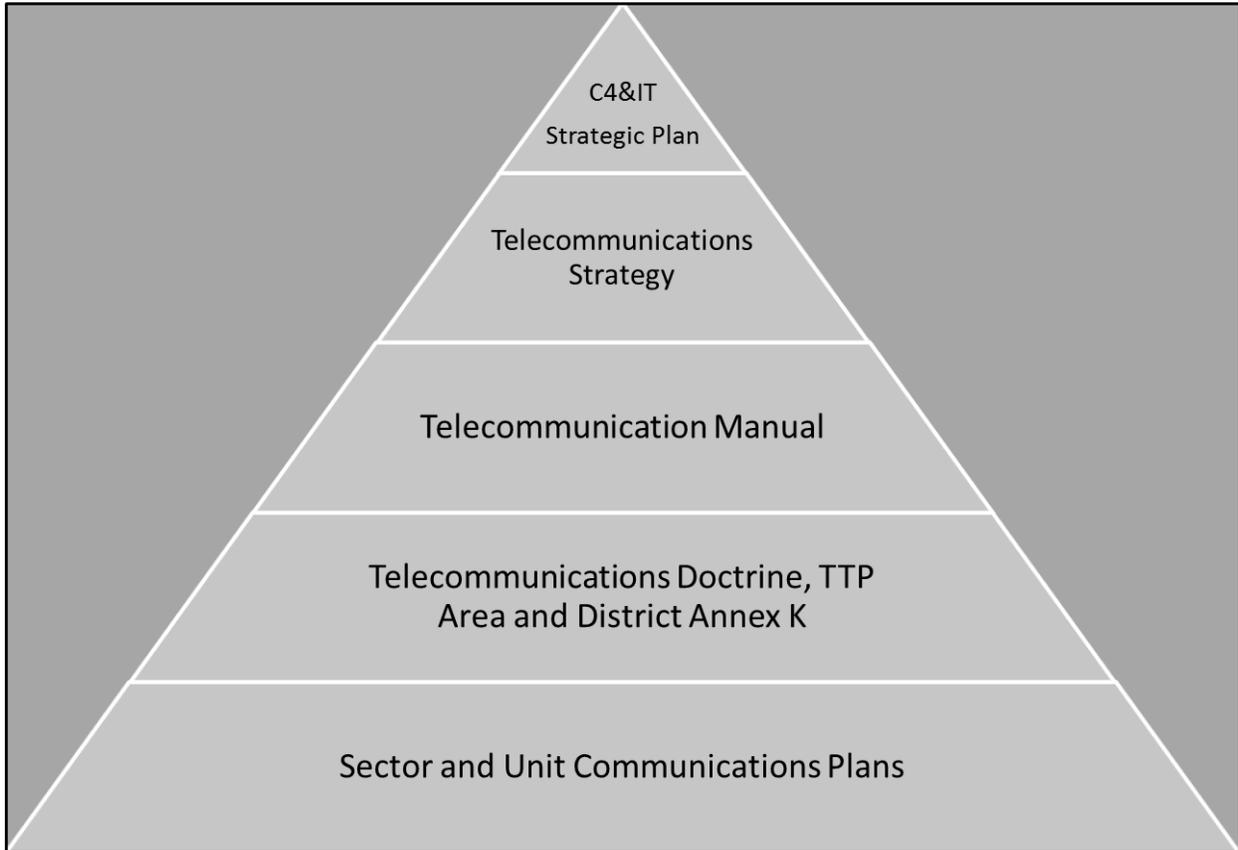
Sustain interoperable communications as per mission requirements. The objective is measured against the ability of individually fielded systems to sustain communications with partner organizations as defined in systems requirements documentation.

**Objective 5.3 – Dynamic scalability**

Field systems for mobile and deployable assets capable of providing on demand increased levels of network service or throughput capabilities with minimal additional effort on the part of the user and/or supporting technical organization. Ultimately this will lead to acquisition and fielding of systems fully capable of sustained on demand throughput. This objective is measured against the ability of fielded systems to meet specific demand thresholds of service as defined in requirements documentation.

**4. Alignment.**

The Telecommunications Strategy serves as the bridge between the overarching C4&IT Strategic Plan and the telecommunications program. It aligns ensuing policies, doctrine and TTPs with governing principals and programmatic goals delineated by the strategy.



**Telecommunication Directives Alignment**

## APPENDIX A Primary Telecommunications Program Governance

Primary Governing Directives	Telecommunications Planning, Requirements and Acquisitions	Telephone, Network, and Satellite Telecommunication Services	Telecommunications Security	Telecommunications Administration	Shoreside Communications	Vessel Communications	Aircraft Communications	Marine Information Broadcasts	GMDSS
14 U.S.C. § 93(a)(15) and (16)	X	X	X	X	X	X	X	X	X
14 U.S.C. § 141	X	X	X	X	X	X	X	X	X
14 U.S.C. § 147	X	X	X	X	X	X	X	X	X
United States, the Communications Act of 1934, as amended (47 U.S.C. §§ 151 et seq)	X	X	X	X	X	X	X	X	X
International Convention for the Safety of Life at Sea (SOLAS), as amended	X		X	X	X	X	X	X	X
International Telecommunications Union (ITU) Radio Regulations	X	X	X	X	X	X	X	X	X
IEC and IALA Standards	X	X	X	X	X	X	X	X	X
Vessel Bridge-to-Bridge Radiotelephone Act (33 U.S.C. §§ 1201-1208)	X		X	X	X	X	X	X	X
Commercial Fishing Industry Vessel Safety Act of 1988, as amended (46 U.S.C. §§ 2101 et seq)	X		X	X	X	X	X	X	X
Assignment of National Security and Emergency Preparedness Communications Functions, EO 13618	X	X	X	X	X	X	X		
USCG Telecommunication Manual (COMDTINST M2000.3 series)	X	X	X	X	X	X	X	X	X
Spectrum Management Policy and Procedures (COMDINST M2400.1 series)	X	X	X	X	X	X	X	X	X
Allied Communication Publication/Joint Army, Navy, Air Force Publication (ACP/JANAP)	X	X	X	X	X	X	X		
Naval Telecommunications Procedures (NTP)	X	X	X	X	X	X	X		
Naval Warfare publications (NWP)	X	X	X	X	X	X	X		
Navy-CG Policy. OPNAVINST 2000.20D/ COMDTINST 2000.9	X	X	X	X	X	X	X		
Homeland Security Presidential Directive 5 (HSPD 5) – DHS/DOD Interoperability	X	X	X	X	X	X	X		
DHS National Emergency Communications Plan – DHS Interoperability	X	X	X	X	X	X	X		
DHS NSSPD 4300 (series) – DHS National Security Systems Policy Directives	X	X	X	X	X	X	X		
DHS Management Directive 1160.1 – DHS Operations Security (OPSEC) Program	X	X	X	X	X	X	X		
DHS CIO C4&IT Strategic Plan	X	X	X	X	X	X	X	X	X
USCG CIO C4&IT Strategic Plan	X	X	X	X	X	X	X	X	X
Information Assurance (IA) policies and directives	X	X	X	X	X	X	X	X	X
Communications Security (COMSEC) policies and directives	X	X	X	X	X	X	X	X	X
Operations Security (OPSEC) policies and directives	X	X	X	X	X	X	X		
Personnel Security (PERSEC) policies and directives	X	X	X	X	X	X	X		

Table A-1

