U.S. COAST GUARD TELECOMMUNICATIONS PLAN (TCP) - DEVELOPMENT DOCUMENT

Deliverable 11

April 28, 1997

Prepared for:
Commandant,
United States Coast Guard,
Washington, DC

Through the:
General Services Administration
National Capital Zone

GSA Contract GS11K94BJD0001
Task Number N1N695003

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Coast Guard Telecommunications Plan (TCP) describes the near to mid-term telecommunications goals and objectives for Command, Control, and Communications (C3) support. It is intended to document internal telecommunications planning and to provide initial guidance on which Coast Guard telecommunications decisions are based. The plan also addresses Coast Guard current and future telecommunications requirements, systems, networks, and capabilities. It also highlights existing operational deficiencies and planned improvements and upgrades.

The Plan, like the Coast Guard Telecommunication System (CGTS), is an evolving document that needs periodic review and revision. The TCP thoroughly documents the current Coast Guard telecommunications architecture, current and future requirements, and technology assessments.

Changes within the organization (i.e., streamlining initiatives, multi-year budget strategies, and cost cutting measures) require accurate program guidance and planning documentation, making this a critical planning document.

Current (Baseline) Telecommunication System

The CGTS has a complex network of interconnected systems that link all Coast Guard facilities (i.e., shore units, aircraft, cutters, boats, etc.). These critical links provide the means to pass voice, data, and video transmissions from facility to facility.

The existing sub-systems provide users with the basic connectivity critical to the baseline system. These subsystems include:

Voice

The TCP identifies several voice communication systems that the Coast Guard uses on a day-to-day basis. They include:

- Telephone
  - Federal Telecommunications System (FTS)
  - Defense Switched Network (DSN)
  - Search and Rescue Telephone (SARTEL)
  - Direct Distance Dialing (DDD)
- Radio
  - Medium Frequency (MF) Distress and Safety System

- High Frequency (HF) Command & Control/Maritime Public Support
- Very High Frequency (VHF) Maritime National Distress System/Short Range Command & Control
- Ultra High Frequency (UHF) Radio
- VHF Direction Finding
- Digital Selective Calling (DSC)

Data

Most of the Coast Guard's mission areas rely heavily on the transfer of information. It is critical that the communication links that transmit and receive this important information meet user requirements. This section discusses the methods or links by which the Coast Guard transmits this data.

- Radio
  - Radio Teletype (RATT)
  - Narrow Band Direct Printing (NBDP)
  - Navigational Telex (NAVTEX)
  - High Frequency Data Link (HFDL)
  - Satellite Communications (SATCOM)
- Landline
  - Coast Guard Data Network (CGDN)
  - Standard Semi-Automated Message Processing System (SSAMPS)
  - Automatic Digital Network (AUTODIN)
  - Secure Data Network (SDN)
  - Teletypewriter Exchange Network (TELEX/TWX)
  - Imagery and Facsimile (FAX)
  - World-Wide Military Command and Control System (WWMCCS)
  - Secret Internet Protocol Router Network (SIPRNET)

  – Anti-Drug Network (ADNET)

Video

Video teleconferencing is divided into three general categories: satellite-based broadcast video teleconferencing, desktop video teleconferencing, and group (large or small) video teleconferencing. Video services may also include video to the desktop in training applications, such as interactive courseware replacing or supplementing “A” and “B” schools. Video teleconferencing offers the potential to significantly reduce travel costs and increase productivity. It is a tool which can greatly improve the work processes between units by offering quick, affordable, and efficient communications. Reductions in travel costs alone will justify the installation of video teleconferencing in many locations.

Contingency Communications

Coast Guard Contingency Communications consist of the following:

- Transportable Communications Centrals (TCCs). These are self-contained communications platforms designed to provide support when temporary communications facilities are required at short notice.

- Other Contingency Equipment. Both CAMS have additional deployable communication systems to support Coast Guard emergency and special operations. These systems include an inventory of:

  – Portable DAMA units (SATCOM)

  – Portable LCCS-300 suitcase (SATCOM Line of Site)

  – Portable INMARSAT “A” Phones (voice only)

- District Contingency Equipment. Each District has a variety of portable communications equipment for contingency operations. Usually it is held at the District/Area COMMCEN and issued as necessary. The following are examples of equipments available from the staffs:

  – ERNIE Modems (2 ea. CODEX 5000, X.500) for dial-up connection to CGDN on CGSW-II

  – Portable VHF Base Stations

  – Portable HF Stations

  – Portable INMARSAT Units

  – Portable DAMA Units

  - Portable LST5s
  - Handheld VHF transceivers
  - Deployable cellular telephones

Systems/Applications

The following major systems and mission essential applications are used by various Headquarters Program Managers to support their mission requirements:

- Aviation Logistics Management Information System (ALMIS)
- Automated Mutual-assistance Vessel Rescue System (AMVER)
- Aids To Navigation Information System (ATONIS)
- Auxiliary Management Information System (AUXMIS)
- Computer Aided Search Program (CASP)
- Fleet Logistics System (FLS)
- Geographic Display Operations Computer (GDOC)
- Joint Maritime Information Element (JMIE)
- Law Enforcement Information System II (LEIS-II)
- Large Unit Financial System (LUFS)
- Marine Safety Network (MSN)
- Personnel Information Management System/Joint Uniformed Military Pay System (PMIS/JUMPS)
- Search and Rescue Management Information System (SARMIS)
- Standard Automation Requisitioning (STAR)
- Supply Center Computer Replacement (SCCR) Project

Future Requirements

The TCP describes all Program Manager future voice, data, and video telecommunications requirements, organized by the distinct interviews with Program Managers and by mission area.

These requirements are prioritized to meet the overall strategy of the Coast Guard including projected mission priorities.

During Program Manager interviews, it was clear that many managers have the vision of future Coast Guard operations. Their vision provided some high level communications requirements. Most of the participants, however, were not able to quantify those requirements in terms of bandwidth which is the range of electrical frequencies a device can handle. In simpler terms, it is the capacity to move information.

Several Program and Support Manager Staffs were solicited for input to the requirements process. As a result, fifteen separate interviews were conducted with various representatives of those staffs. Replies to prepared questions, ranging from general solicitations on future views of the Coast Guard's general needs for communications services to specific inquiries about system bandwidth requirements, ran the gamut: validated requirements, not validated requirements, and solutions. Interviewee responses were further refined into requirements that could be validated in the concurrent clearance process. The reports, on each of the interviews, are on file with the Commandant (G-SCT) staff.

The following Program Managers were interviewed: G-A, G-CFP, G-L, G-M, G-OC, G-OP, G-SE/SLS, G-SEA, G-SC, G-SI, G-WK, G-WP/WT

Future telecommunications requirements are listed in the TCP by Program and later in priority order by mission. The following is a prioritized list of those requirements beginning with the requirement considered the most important:

1. Automated Systems/One Time Data Entry
2. Network-of-Networks
3. Formal and Informal Message Delivery
4. Centralized Data Storage and Access
5. Data Security
6. Video & Imagery
7. Interoperability
8. Remote Access (dial-in)
9. World-wide internal access to Critical CG DB & Applications
10. Mobile Communications
11. Automated Chart Updates

12. World-wide Public Access to Coast Guard Databases
13. Provide Navigation Information Service
14. Short Range Radio Communications
15. Satellite Communications
16. Solution to Cutter Antenna Interference Problem
17. User Pull
18. Consolidated Management Reporting System
19. Direction Finding Capabilities
20. Video Teleconferencing
21. Telecommuting
22. Open Systems Architecture
23. Digital Signature Standard
24. Telemedicine Capability
25. User Charge-back
26. Global Dial-tone

These requirements were compared to the Baseline Architecture and with the gaps identified in the C4I Baseline Architecture Document. Each of these requirements relates to one or more of the critical gaps which are listed in Section 3.7 of the TCP, and reference is made to the gap which most closely relates to the requirement. The critical gaps, in Section 3.7, directly relate to gaps identified in the C4I Baseline Architecture Document.

The Telecommunications Plan and the C4I Baseline Architecture and Plan are related in many areas, and synergy was obtained by ensuring that these efforts were completed hand-in-hand. Significant input, to the development and preparation of the Program Manager Interview questions, was obtained from drafts of the C4I Baseline Architecture document. The C4I document identified critical gaps in capabilities. These gaps correlate directly to many of the future requirements addressed in the Telecommunications Plan. The focus of the Telecommunications Plan differs from the C4I Baseline Architecture in that it is limited to communications requirements, but it addresses these requirements throughout the Coast Guard. Accordingly, the Telecommunications Plan incorporates several programs not addressed by the C4I efforts, particularly administrative and support. For this reason, not all requirements, in the Telecommunications Plan, will link directly to the critical gaps discussed in the C4I documents.

The following gaps between the TCP baseline architecture and the future requirements were identified. The process established the framework for an assessment of relevant technologies and recommended solutions. The resulting list shows the most critical gaps in Coast Guard communications capabilities. These gaps include:

- Communications Connectivity
- Maritime Public Support
- Interoperability
- Information Exchange
- Data Security
- Decision/Tactical Support
- C3 Systems

All of the requirements and gaps involve movement of data into, out of, and within the Coast Guard. Most of that movement requires a Wide Area Network (WAN) with the ability to connect with all Coast Guard entities. One significant task is the determination of the volumes of data that must move concurrently on the circuits at any point in time. This problem has been compared to liquid transportation through pipelines. The data problem is sometimes referred to as “sizing the pipes.” The whole process is important, since the cost of the network is very much related to the “size of the pipes” to all Coast Guard personnel.

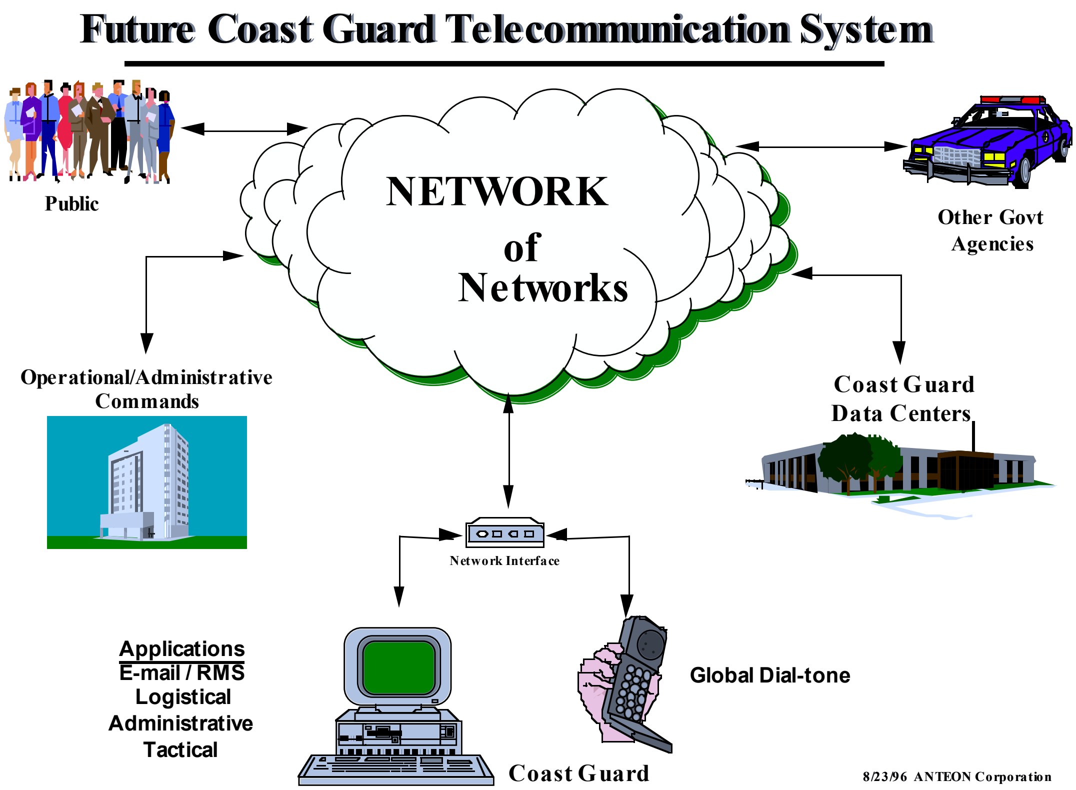
Different legs of the network may require different magnitudes of data flow. The requirements for a Coast Guard WAN are an accumulation of all the requirements from Coast Guard applications producing data for movement within the organization. There are only two program/application managers who have produced detailed quantified studies of their data communication requirements. They are G-W for the Personnel Management Information System II (PMIS II) and G-S for the Fleet Logistics System (FLS).

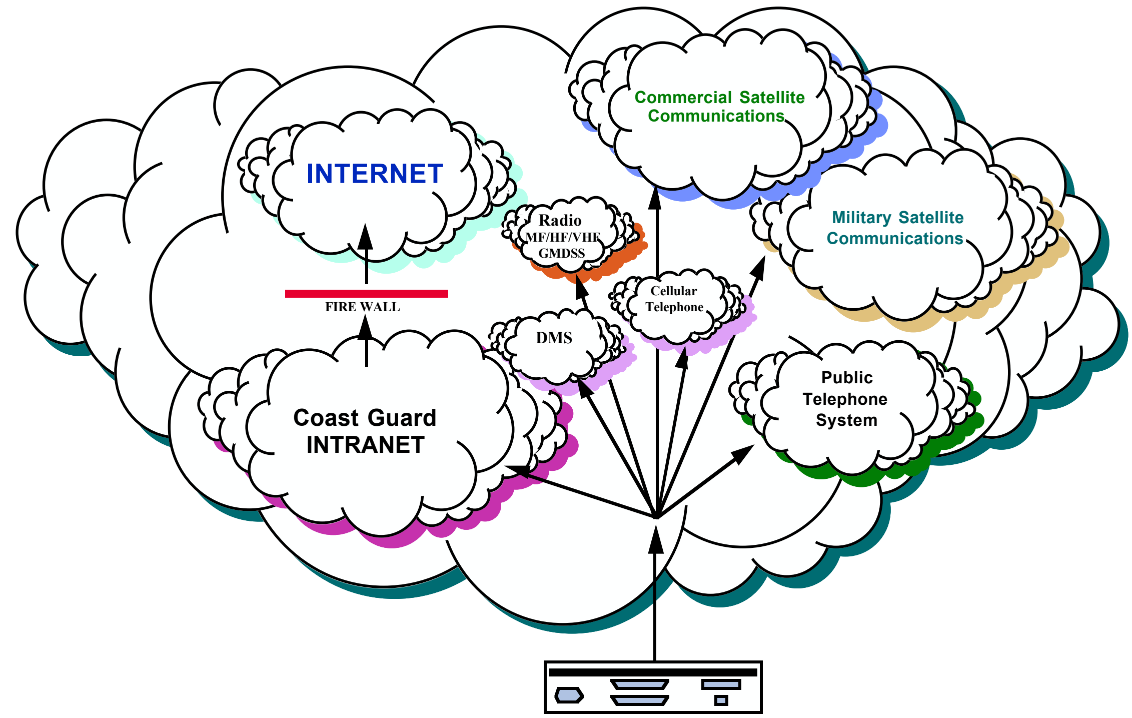
An estimate of the peak bandwidth that communications circuits at OSC Martinsburg will be required to support is approximately 2200 kbps. This is equivalent to about one and one-half T1 circuits.

Network-of-Networks

On the following page, is a user’s perspective of the network of the future. Users will use one telephone to meet all voice requirements and one workstation to meet all data and video needs. The network itself will be transparent to the user who will be connected to the network by an intelligent gateway. The gateway will automatically select the best path from originator to addressee, depending on the type of service (i.e., voice telephone calls, record message traffic, applications, etc.) and based on whether the call is a voice, data, or video transmission. The Network-of-

Networks is the vision of the future (10-15 years). Technology is not currently available to implement all aspects of this all-encompassing networking solution. However, technology is in place or will be in place in the next 5 years to implement significant portions of this vision.





Gateway to the "Network of Networks"

Technology Assessment

After accomplishing two very important tasks, documenting the baseline architecture and developing a comprehensive list of future telecommunications requirements, several technology areas were assessed. These were (1) Data Networking, (2) Mobile Communications, and (3) Requirements for Interoperability with DoD. The networking technologies were analyzed at a high level to determine their potential for addressing current and future requirements, and their impacts on the Coast Guard's future architecture.

Data Networking

Several data networking technologies were identified that showed potential for meeting the Coast Guard's current and future data networking requirements. These technologies, which encompass both dedicated and on-demand networking connections, include X.25, Asynchronous Transfer Mode (ATM), Frame Relay, Integrated Services Digital Network (ISDN), Point-to-Point networking services, and Very Small Aperture Terminal (VSAT) networking. Also important in the planning for the future network architecture is the Defense Message System (DMS), which will have a considerable impact on the Coast Guard's data networking solution.

Initial cost estimates, which include installation charges and basic monthly rates, along with equipment purchase costs, were determined using a sample network configuration consisting of two remote units (Atlantic and Pacific Area) connected to a central site (OSC Martinsburg). This limited network architecture was considered adequate for high-level cost comparison purposes.

Mobile Communications

Several wireless networking alternatives were analyzed, including High Frequency (HF) and Satellite Communications (SATCOM) point-to-point communication technologies and services. These technologies include the following:

- Spread-Spectrum Packet Radio
- Low Earth Orbit Satellite (LEOS) System (i.e., Iridium, Globalstar)
- Regional Satellite System (i.e., AMSC)
- International Maritime Satellite (INMARSAT)
- Very Small Aperture Terminal (VSAT) (DirecPC)
- Military Satellite Communications (MILSATCOM)
- Cellular Networks (i.e., Standard and CONDOR capable cellular service)
- Traditional High Frequency (HF) Wireless Communications
- Tactical Defense Message System (DMS)

DoD Interoperability

The Coast Guard operates in a multi-mission environment which includes increasing requirements to participate in combined operations with DoD. One factor critical to continued mission success, improved readiness, and enhanced quality of life for mobile forces will be the ability to share information, seamlessly, and in real-time or near real-time through flexible, adaptable, interoperable communications systems.

The current communications systems will not meet the throughput demands of the future. However, taking a "Networks-of-Networks" approach will lead to the fielding of communications assets that are inter-operable and flexible enough to meet the throughput demands of today's and tomorrow's Coast Guard operational units.

Several technologies were explored and analyzed at a high level to determine their potential for addressing current and future requirements, and their impacts on the Coast Guard's future telecommunications architecture.

It was determined that several current and emerging telecommunications technologies, each with unique capabilities, will be used in conjunction with one another to make up the future "Network-of-Networks". This all encompassing system will move all types of information seamlessly from place to place within the Coast Guard and also interface with other government agencies through direct circuits and network gateways. Some of these technologies are already in place and in operation, some will be the result of future procurements, and others will be provided to the Coast Guard by DoD to promote interoperability, and support the requirement for Coast Guard/Navy compatibility.

For record message traffic and electronic mail delivery, and providing the transport medium for mission essential applications, the "Network" will provide access to the following basic services:

- Dedicated DoD Networks (i.e., Defense Information System Network (DISN), Integrated Tactical/Strategic Data Network)
- Defense Message System (DMS)
- Electronic Mail Exchange
- MILSATCOM
- Electronic Data Interchange
- Defense Satellite Communications System (DSCS)
- Global Broadcast System (GBS)
- Cellular Telephone
- Regional Satellite Systems
- INMARSAT
- Traditional HF Communications Systems
- Digital Modular Radio System
- Integrated Terminal Program
- Automated Digital Network

Technology Alternatives

With consideration given to capability limitations and/or operating costs, there is no specific technology that will meet all Program Manager needs. However, by carefully selecting, analyzing, and combining several technologies into one all encompassing "Network-of-Networks," and thus allowing them to complement and enhance each others' capabilities, a comprehensive networking solution was developed.

The TCP presents a high level view of several possible networking solutions. Each alternative solution is based on an initial capabilities assessment, technology availability, and cost analysis.

Each alternative contains a mix of data, mobile, and interoperability technologies, which together produce a networking solution to meet all voice, data, and video communications requirements.

Other systems, not listed as an integral part of the networking alternatives, such as DISN, were investigated as possible networking solutions during the high-level technology analysis. These systems were not considered to be viable solutions due to one or more outstanding deciding factors. These include costs, bandwidth availability concerns, priority allocations constraints, and responsiveness to Coast Guard needs.

The table on the following page shows the technologies selected for each networking alternative to form a hybrid networking solution that will meet all Coast Guard voice, data, and video service requirements:

Alternative	Systems and Units	#1	#2	#3
Data	CGDN+ Tier 1 Backbone	Point-to-Point	Point-to-Point	ATM
	CGDN+ Tier 2	Frame Relay	VSAT	
	CGDN+ Tier 3/4	Dial-up ISDN	VSAT	ISDN Dial-Up
	Tactical DMS to 378's/270's, DOD trfc for all others	DMS Gateways	DMS Gateways	DMS Gateways
	Tactical/record msg trfc to 378's/270's, LMCG to 210s	MILSATCOM	MILSATCOM	MILSATCOM
	MEAs to all units	Commercial SATCOM - Regional Satellite - Inmarsat	Commercial SATCOM - VSAT - LEOS	Commercial SATCOM - LEOS
	GMDSS reqt/sat backup to mobile units, HFDL WPB/WLB	MF/HF Radio Comms	MF/HF Radio Comms	MF/HF Radio Comms
	Public	INTERNET	INTERNET	INTERNET
Voice	Shore ops/mobile, distress/C3	VHF-FM	VHF-FM	VHF-FM
	GMDSS reqt/sat backup	MF/HF Radio Comms	MF/HF Radio Comms	MF/HF Radio Comms
	Tactical voice on 378/270's	MILSATCOM	MILSATCOM	MILSATCOM
	Admin and C3 voice for shore and mobile units	Commercial SATCOM - Regional Satellite - Inmarsat	Commercial SATCOM - LEOS	Commercial SATCOM - LEOS
	Emerg, admin and C3 comms for shore and mobile units	CONDOR	Cellular Service	CONDOR
Video	All units with terrestial connection	PSTN	PSTN	PSTN

The first alternative is a network configuration based primarily upon proven, currently available technologies with minimum developmental risk. It consists of several data and voice technologies that combined will meet all record message, mission essential application, and tactical communications needs. These technologies include Point-to-Point and Frame Relay technology, with ISDN dial-up capabilities where needed; and MILSATCOM, Commercial SATCOM, and traditional MF/HF for wireless communications support.

The second alternative is based upon high-probability of success technologies being deployed in the near future. (These technologies are anticipated to provide significant opportunities to improve Coast Guard communications processes.) This alternative is similar to Alternative 1, however, SATCOM is used more extensively to meet shore-side and wireless communications requirements.

The third alternative includes other potential high impact technologies, such as ATM, which are available or anticipated and have not been considered in Alternative 1 or 2.

Recommended Future Architecture

Having carefully reviewed each of these alternatives the Coast Guard selected two networking solutions for complete analysis.

In short, the analysis considered the following elements: cost/benefit, engineering feasibility, stakeholders, resource savings, time and ease of implementation, risk, trade-off (cost/time/performance), and force field analysis (weighing issues for and against migration to a new system).

The following alternatives were selected by the Coast Guard for further analysis.

- Alternative 1: includes a combination of Point-to-Point and Frame Relay networking technology, using T1 circuits running TCP/IP, for data communications, with ISDN services added to the lower tier network, where available and unique requirements dictate. Wireless communications requirements are met with a hybrid network of MILSATCOM, commercial SATCOM, and traditional MF/HF radio communications. Specialized cellular telephone services (i.e., CONDOR) will be used for high priority clear and secure voice and data communications, and will be available, as a backup, to meet operational and administrative communications requirements.

  The above combination of data and voice technologies will meet all record message, e-mail, mission essential application, tactical communications, and video teleconferencing needs.

- Alternative 2: combines Point-to-Point networking technology with commercial Very Small Aperture Terminal (VSAT) SATCOM services to meet all shoreside data communications needs. Wireless communications requirements are met with MILSATCOM, commercial Low Earth Orbit Satellite (LEOS) services, and traditional MF/HF radio communications. Alternative 2 is based upon current and high-probability of success technologies being deployed by other enterprises in the near future. (These technologies are anticipated to provide significant opportunities to improve Coast Guard communications processes.) This alternative is similar to Alternative 1. However, commercial SATCOM is used more extensively, in Alternative 2, in order to meet shore-side and wireless communications requirements.

  If the new systems and technologies mature as expected, Alternative 2 will meet the Coast Guard's requirements as well as Alternative 1.

- In addition to the two alternatives discussed above, ATM technology was also analyzed as a possible wide area network (WAN) solution. This evaluation was accomplished by comparing network (Tiers-1 and 2) solutions in each of the three WAN technologies.

Alternatives 1 and 2, and ATM were analyzed to determine the cost and engineering feasibility of future implementation. Each alternative included several technologies that are already in use and supported by the Coast Guard. Although these technologies are an integral part of the future network, they do not impose an impact on either the cost of implementation or the operation of the new system. Therefore, they are considered to be a "constant" factor, and were not included in the life cycle costing of the new network. Technologies that are new or will otherwise impact the cost of implementation or operation of the new system were included in the LCCE.

Final Recommendation and Migration Plan

A final recommendation for network design was concluded after a close examination of all available technologies, and detailed discussions with Coast Guard network planners and engineers. This recommendation is based on cost, availability and reliability factors, open systems compliance, and network improvement initiatives currently in progress (i.e., Coast Guard Data Network (CGDN) Plus).

The selected internetworking architecture applies to all Coast Guard mission areas and will meet all voice, data, and video requirements. This architecture was developed from detailed analysis of data, mobile, and interoperability technologies, and input received from Program Managers and key Coast Guard personnel during TCP development.

The architecture for the data segment of the Coast Guard Network-of-Networks, known as CGDN Plus, is based upon proven technologies with minimum developmental risk. It was chosen because it is currently the most flexible and scaleable network. As technology changes, the network can be quickly changed to meet customer requirements. In the future, certain economies of network cost may be realized through the use of other technologies. Consequently, the business case may result in a hybrid network.

Several other new technologies, which are needed to achieve the future network architecture (year 2003), such as LEOS and specialized cellular service (CONDOR), are expected to be available in 1998. However, the Coast Guard should not commit to implementing new technology until it has been thoroughly tested and operated commercially for a reasonable period of time.

To allow for this, we have developed a three-phased approach to implementation of the new network, as described below.

- **1998**
  - ✧ T1 Point-to-Point connectivity on the Coast Guard Data Network.
  - ✧ ISDN or FTS2000 dial-up services to meet unique requirements.
  - ✧ Connect to DMS via strategically located DMS gateways.
  - ✧ Commercial Satellite services for world-wide mobile coverage at the least cost.

- ✧ MILSATCOM for primary ship-shore message traffic delivery.
- ✧ Traditional MF/HF Radio Communications will continue to be available, on a limited basis, to provide ship-to-ship, ship-to-shore, and air-to-ground voice communications (i.e., SAR and L/E operations, etc.).
- ✧ INTERNET for public access to Coast Guard information via "home pages".
- ✧ VHF-FM for maritime public support.
- ✧ Cellular Telephones for high priority communications, and as a backup system for administrative and operational voice communications within the CONUS and portions of the CONUS Exclusive Economic Zone (EEZ) for land-based mobile units.
- ✧ Public Switched Telephone Network (PSTN) to meet video requirements. This can be arranged on an "as needed" basis which minimizes the recurring costs of leased lines.

- **2000**

  The following changes/enhancements may be made to the "network" in the year 2000:

  - ✧ T1 Point-to-Point backbone circuit connecting major Coast Guard units (i.e.., Headquarters, Areas, MLCs, Districts)
  - ✧ Frame Relay connecting all smaller Coast Guard units.
  - ✧ ISDN/FTS2000/VSAT to meet unique requirements not met by the Frame Relay network.
  - ✧ Specialized Cellular Service may be used in lieu of standard cellular service. Dual mode secure cellular/satellite services, with broadcast capabilities, are expected to be available from multiple vendors by the year 2000.

- **2003**

  Should the Coast Guard decide to accept Frame Relay, or other new networking technology, in the year 2003, the following changes may be made to the Coast Guard "network":

  - ✧ Frame Relay will link together all Coast Guard units and will allow for technology insertion which will, in turn, allow the telecommunications system to take advantage of new technology over time.

- Commercial SATCOM (LEOS system) may replace regional satellite and geostationary INMARSAT services for meeting special purpose mobile voice and data communications requirements.

The example architecture provides a comprehensive networking solution capable of meeting all of the Coast Guard's current and future telecommunications requirements. It provides the ability to quickly and easily shape information into knowledge, and is designed to be flexible, configurable, and scaleable. The architecture consists of several telecommunications technologies that will best meet the Coast Guard's current and future telecommunications requirements with the least cost and risk.

Factors considered in the selection of Point-to-Point technology for the new data network are:

- **Availability:** T1 Point-to-Point technology was readily available for rapid and least risky implementation during the just-in-time installations of CGSWIII (June 96 to September 97).

- **Flexible and Scaleable:** Point-to-Point technology provides a flexible and scaleable networking solution.

- **Open Systems Compliant:** Point-to-Point technology, using Open Shortest Path First (OSPF) routing protocol, is non-proprietary and meets government open systems requirements.

- **Speed:** T1 Point-to-Point technology will provide a significant circuit capacity improvement over the current 56 kbps backbone network and will meet all current and future Coast Guard voice, data, and video requirements.

- **System Engineering:** Point-to-Point technology implementation requires the least up-front engineering of the available technologies (i.e., Frame Relay, ATM, SONET, etc.)

If the Coast Guard should decide to use Frame Relay services in the future, major factors which may be considered in the selection of Frame Relay over Point-to-Point, at that time, may be:

- **Speed:** Frame Relay has a more granular speed capability. This means that it has the capability to have a defined Committed Information Rate (CIR), which allows a connection speed to be defined in smaller increments than Point-to-Point can provide.

- **Virtual Circuits:** Frame Relay has the capability to define Permanent Virtual Circuits (PVCs). This allows the customer to define PVCs between the various site locations as multiple singular circuits are installed to the Frame Relay "cloud." The "virtual" circuits allow more efficient use of the network, by providing high volume paths.

- **Cost:** In the future, Frame Relay may be less costly to install and operate than Point-to-Point. By taking advantage of the CIR capabilities, excessive and wasted bandwidth can be eliminated. After a usage history is established, the most cost effective bandwidths can be chosen, which will reduce overall costs.

- **More Flexible and Scaleable:** Due to dynamic CIR and PVC capabilities, future Frame Relay networks may be "tuned" much easier and faster than Point-to-Point. This means that the CIR can be quickly modified to provide more or less bandwidth, as required, between site locations.

Training

- **Data Network**: Operator training for the data network is commercially available. Technical system decisions have enabled the current base of X.25 knowledge to be easily adapted to Point-to-Point networks.

- **DMS**: The DMS implementation plan is still incomplete and final decisions have not yet been made on training availability.

- **MILSATCOM**: The Coast Guard is familiar with the operational and technical aspects of several military and commercial satellite communication systems, and training in some of these areas is already in place.

- **Specialized Cellular Service (CONDOR)**: Training for specialized cellular service capabilities will be available from commercial service providers.

Recommendation

The current networking initiative, CGDN Plus, should continue, as it will provide the most capable and cost effective solution to meet Program Manager requirements. The installed base will include all major and some smaller units by 1 September 1997.

Technology is changing at an extremely fast pace. With this in mind, the Coast Guard should consider implementing state-of-the-art technology (i.e., Frame Relay, ATM, SONET, etc.) by the year 2003, when a technology refreshment will most likely be needed. Frame Relay, for example, provides added levels of flexibility and scaleability, along with its own network management services, and may yield lower annual costs than Point-to-Point. The costs are very dependent on the selected Committed Information Rates (CIRs) at all units.

To provide connectivity to shore units where Frame Relay access is not available, ISDN, FTS2000 dial-up, or VSAT services could be used.

As DMS implementation comes to fruition, gateways, possibly located at several sites, such as OSC Martinsburg and the two Areas, will provide Coast Guard shoreside access to DMS. Ships may be linked to DMS over MILSATCOM which is expected to continue to be the primary means for ship-shore record message delivery.

Gateways to the INTERNET may be located at several locations. These sites may be Headquarters, OSC Martinsburg, and an additional site on the west coast. All Coast Guard access to the INTERNET should be via these sites, where appropriate safeguards will be provided to protect Coast Guard internal systems from unauthorized access. Additional gateways at other locations may be required as INTERNET access requirements increase over time.

Regional Satellite services and INMARSAT should continue to be available with coverage of the CONUS and coastal maritime areas for shore-based and mobile Coast Guard units when needed. After which, LEOSs will greatly expand the available coverage areas by offering service everywhere on Earth, including the polar regions where current satellite services cannot reach. LEOSs will also eliminate the requirement for stabilized dish antennas on mobile platforms. Increased competition may decrease costs of the current system.

Traditional MF and HF radio communications will continue to be used primarily as a backup system for satellite equipped vessels. It will also be needed to meet certain GMDSS requirements, and to maintain Coast Guard-Navy compatibility, as the Navy plans to continue its use of traditional radio communications into the next millennium.

VHF-FM communications may be augmented or replaced by emerging technologies sometime in the distant future. However, until then, VHF-FM will continue to be used to meet National Distress System (NDS), Global Maritime Distress and Safety System (GMDSS), and Coast Guard command and control requirements, as stated in Chapter 3.

Interoperability is a major benefit of specialized cellular service (CONDOR) which is expected to provide several enhancements over traditional wireless communications. Its secure (FORTEZZA card), dual mode (cellular/satellite) capability will provide mobile units with reliable world-wide voice and data connectivity. CONDOR's voice broadcast mode will provide an "all call" feature similar to the capability currently found in most traditional radio communication systems. Initial equipment and service costs will likely be high, as vendors recoup research and development costs. However, costs are expected to decline as multi-agency use of CONDOR increases.

Video requirements, for the foreseeable future, can be met using dial-up services via the Public Switched Telephone Network (PSTN). This will ensure the best possible service at the least cost to the user. PSTN dial-up services can be arranged on an "as needed" basis, which minimizes the recurring costs of leased lines.

It is important to keep in mind that costs and solutions available may vary depending on the geographic area. For example, equipment and circuit costs in "out of CONUS" areas (i.e. Alaska, Hawaii, Guam, FESEC, Caribbean) may be significantly higher than in CONUS, and the networking solutions available may be limited.

1. INTRODUCTION

1.1 Purpose

The Coast Guard Telecommunications Plan (TCP) encompasses all Coast Guard current and future voice, data, and video telecommunications requirements. The Plan is designed to be dynamic and will be updated as often as needed to keep pace with rapidly changing technology and user requirements.

The Plan, as the governing Coast Guard telecommunications planning document, also presents a high level view of telecommunications goals and strategies. It is the source for stating telecommunications requirements and developing detailed plans to satisfy those requirements.

1.2 Scope

This Plan addresses validated Coast Guard current and future telecommunications requirements, systems, networks, and capabilities, with a high level discussion of existing operational deficiencies and planned improvements and upgrades. The Plan focuses on data, mobile, and interoperability technologies to meet shore, afloat, and airborne telecommunications requirements.

The TCP makes no distinction between operational and administrative telecommunications. These activities are completely integrated with priorities determined by the overall need for timeliness and the criticality of information transfer. The TCP describes telecommunications requirements and the current (baseline) system's operations and resources. This description includes communication stations and centers, radio frequency circuits, local and wide area networks, and shipboard systems. It details the orderly evolution of existing networks and systems into a flexible and scaleable Coast Guard Network-of-Networks.

The requirements for and the descriptions of the communications links that support other types of systems (e.g., automatic data processing (ADP), intelligence, radio navigation, decision support, sensors, etc.) are included. However, detailed information related to these types of systems is beyond the scope of this document.

1.3 Objectives

The Coast Guard Telecommunications System (CGTS) must provide a rapid, reliable, and secure means to exercise the command and control of mobile and fixed (shore-based) units in a cost effective manner. It must also provide a means for merchant shipping, maritime interests, and the boating public to communicate reliably with the Coast Guard on allocated frequencies. In addition, the system will provide rapid, reliable, and secure means by which other Federal agencies, particularly the U.S. Navy, can communicate with the Coast Guard and its operating forces in support of their respective missions.

1.4 TCP Organization

The TCP is organized in a logical, non-technical, and easy to understand manner beginning with a high level description of the current Coast Guard telecommunication system. This is followed by a detailed description of Headquarters Program Manager voice, data, and video requirements in the future. Once the future requirements are captured, the TCP documents an analysis of available and emerging technologies capable of meeting these requirements. It concludes with a recommendation for a future, all-encompassing Coast Guard Network-of-Networks, including a high level migration plan.

2. Telecommunication Architecture Baseline

2.1 Introduction

In this chapter we describe the current state architecture "As-Is" for the Coast Guard Telecommunications System (CGTS). Our discussion covers all of the key equipment and services that make up the overall baseline system architecture. We have dissected the system into three major components: voice, data, and video.

In the following sections we will describe the key systems within each major component and each of their corresponding applications.

2.2 System Description

The CGTS has a complex network of interconnected systems that link all Coast Guard facilities (i.e., shore units, aircraft, cutters, boats, etc.). These critical links provide the means to pass voice, data, and video transmissions from facility to facility.

The existing sub-systems, we have listed below, provide users with the basic connectivity critical to the baseline system. We have included diagrams and descriptions of all relevant Coast Guard unit types that rely on the CGTS, and a listing of their required equipment and software.

2.2.1 Voice

We have identified several voice communication systems that the Coast Guard uses on a day-to-day basis. They include the following:

2.2.1.1 Telephone

The Coast Guard takes advantage of several systems for telephone communication services. In recent years they have employed cellular technology to meet their growing demands. The following systems and services currently support the Coast Guard's telecommunication needs.

- **Federal Telecommunications System (FTS)**: FTS provides telephone communications to the Coast Guard through a leased inter-city network that the General Services Administration (GSA) established. The Coast Guard relies on FTS2000 to fulfill their primary telephone system requirements. The Coast Guard receives additional telephone service from commercial systems to supplement FTS2000. FTS2000 supports both local and long distance service.

- **Defense Switched Network (DSN**): The DSN is the primary provider of long distance communication service for the Department of Defense (DoD). Automatic Voice Network (AUTOVON) is a sub-set of the DSN and it provides an interface between Coast Guard echelons and other DoD agencies for the purpose of military preparedness.

- **Search and Rescue Telephone (SARTEL)**: SARTEL provides immediate and uninterruptable voice communications through various hotlines. This system meets Coast Guard needs by providing a communication link that coordinates time critical operational SAR missions.

- **Direct Distance Dialing (DDD):** DDD is a commercial long distance telephone service that the Coast Guard uses when FTS is not available.

2.2.1.2 Radio

The Coast Guard uses many types of radio systems and frequencies to support their various mission areas. In the following sections, we discuss the components that make up the radio portion of the CGTS.

- **Medium Frequency (MF) Distress and Safety System:** The Coast Guard provides distress monitoring, marine safety and weather broadcasts, and command and control communications out to at least 70 nautical miles offshore. The CGTS provides coverage within the practical limitations of each district's geographic area.

  This system consists generally of Single Side Band (SSB) guard receivers tuned to 2182 kHz supported by multi-channel transceivers for working frequency operations. Coast Guard Group Offices provide the primary monitoring points for this voice transmission system. Coast Guard ships are equipped with suitable 2182 kHz radio guard capability, while they are underway. Aircraft are also similarly equipped to transmit and receive as required on SAR missions.

- **High Frequency (HF) Command & Control/Maritime Public Support**: The Coast Guard uses HF (3-30 MHz) voice communications for command and control to assist in the execution of SAR responsibilities beyond MF coverage. HF is their primary long haul voice communication system between shore locations and underway vessels and aircraft. They may transmit classified information via HF radio using voice security equipment to protect classified and official use only transmissions.

  The Coast Guard has installed HF radio equipment on their cutters as well as selected boats and aircraft. Large cutters usually have multiple channel HF transmit and receive capabilities while limited capabilities may be installed on other units.

  The primary shore facilities who support these HF frequencies are Communication Stations (COMMSTAs). Most ships and all aircraft also have this capability. Other selected Coast Guard shore units, including Air Stations and Groups, use HF radio for direct voice communications with their operational platforms.

  They also use HF (voice) to support the Automated Mutual Assistance Vessel Rescue System (AMVER) program and navigational safety on the high seas.

In addition, Marine Information Broadcasts (MIBs), consisting of various types of Notices to Mariners (NTMs) and high seas weather information, are transmitted using Voice Broadcast Automation (VOBRA) equipment and software with a Coast Guard developed Automated Broadcast Scheduler (ABS). The combination of VOBRA and ABS allows for hands-off operation (preparation and transmission) of all MIBs.

Very High Frequency (VHF)—Maritime/Short Range Command & Control: The Coast Guard operates the National VHF Distress System on the maritime mobile band (≈ 156 MHz). They designed this system to provide distress calling, marine safety information broadcasts, and command and control coverage out to 20 nautical miles offshore. Numerous Coast Guard shore units require VHF capabilities to accomplish their missions. These include Groups, Small Boat Stations, Air Stations, Vessel Traffic Service (VTS) sites, some COMMSTAs, and Marine Safety Offices. Group commanders maintain guard receivers on Channel 16 (156.8 MHz), along with the capability to shift to several working frequencies as needed. The Coast Guard has also equipped their vessels and aircraft with transceivers, so they may guard Channel 16 and other required VHF frequencies. Some of these platforms also carry hand-held VHF radios for use by boarding parties and other special activities.

For short-range command and control, the Coast Guard is using the maritime band (~ 156 MHz). This system is protected with Data Encryption Standard (DES) devices and provides the Coast Guard with a private voice network for the control of forces. It also allows for seamless interoperation with law enforcement agencies like Customs, Drug Enforcement Agency (DEA), and the Federal Bureau of Investigation (FBI).

In addition to VHF-FM, the Coast Guard employs and guards receivers for VHF-AM (on 121.5 MHz). They use this system primarily for air stations, ships, and aircraft.

- **Ultra High Frequency (UHF) Radio**: The Coast Guard uses UHF radio communications for air-to-ground voice communications. They have equipped all of their aircraft with this capability to support Coast Guard missions and to meet air traffic control requirements. Additionally, air stations and some selected cutters maintain UHF radio equipment for connectivity with these Coast Guard airborne resources.

- **VHF Direction Finding:** Many units in the Coast Guard have direction finding capabilities. This system provides a significant adjunct to the national VHF distress system in limited geographical areas. Triangulation methods are used, in many locations, to determine the approximate location of vessels in distress.

- **Digital Selective Calling (DSC):** As part of the world-wide implementation of the Global Maritime Distress and Safety System (GMDSS), DSC automation procedures are being added to the MF, HF, and VHF radio systems ashore and afloat. DSC is an alerting and radio circuit establishment feature that enables automatic initialization of communications between transmitters and receivers. (It is analogous to dialing a telephone number over the commercial telephone system.) Stations are notified of incoming traffic when their communications equipment receives the DSC data stream. International agreements require all SOLAS vessels to be capable of DSC operation on all of their radio communication systems not later than February 1999. Coast Guard aircraft must also have this capability to establish contact with commercial ships. The automatic nature of DSC operations will affect both radio operations procedures and personnel requirements.

2.2.2 Data

Most of the Coast Guard's mission areas rely heavily on the transfer of information. It is critical that the communication links that transmit and receive this important information meet user requirements. This section discusses the methods or links by which the Coast Guard transmits this data.

2.2.2.1 Radio

The following methods are used by the Coast Guard to send and receive data through radio transmissions.

- **Radio Teletype (RATT)**: Deployed Coast Guard ships and aircraft receive record message traffic through both broadcast and ship-to-shore circuits by means of HF RATT. This allows these deployed units to communicate with a COMMSTA, who acts as the shore or ground teletype guard station. The Coast Guard uses RATT for transmitting distress, weather, and other operational and administrative traffic. They use either point-to-point or broadcast mode to transmit this traffic between shore locations and underway ships, aircraft, and other shore units.

  The shore commands can send their record traffic to the deployed units by forwarding messages to the appropriate COMMSTA. They can do this via landline. The COMMSTA can then deliver the message to the unit over the appropriate RATT circuit.

- **Narrow Band Direct Printing (NBDP)**: Simplex Teletype Over Radio (SITOR)/NBDP is a part of the replacement for the Morse Code (CW) systems under GMDSS. Some selected COMMSTAs already provide NBDP maritime information broadcasts in addition to their normal communications commitments. SITOR is the current international standard for maritime data communications on HF, as is Navigational Telex (NAVTEX) (discussed below).

  NBDP provides the capability for transmission of information over HF radio in data format. It operates in two modes: simplex and duplex. Almost all COMMSTAs have the equipment to support both operation modes. The Coast Guard uses half-duplex mode for all two-way ship-to-shore data communications. They use simplex mode for NAVAREA notices, hydrographic notices, and weather broadcasts.

In simplex mode (one-way broadcasts), NBDP employs an error detection and correction method known as Forward Error Correction (FEC). In duplex mode, NBDP employs a method called Automatic Repeat Request (ARQ). Both of these modes result in virtually error-free reception.

- **Navigational Telex (NAVTEX)**: NAVTEX is another key part of the replacement for CW under GMDSS. This is an automated radio system used by the Coast Guard to broadcast urgent Search and Rescue (SAR) and medical information, and navigational and other marine warnings/information. They do this via a digital format on 518 kHz. NAVTEX is one of the current international standards for maritime data communications on medium and high frequencies.

- **High Frequency Data Link (HFDL)**: The HFDL is a polled, packet-switched, wide-area data network that operates over HF radio. The Coast Guard uses HFDL primarily for passing both unclassified and classified operational and administrative record message traffic to non-telecommunication specialist staffed vessels (i.e. WLBs and WPBs).

  Underway HFDL cutters are electronically queried in sequence by the master station (COMMSTA) to determine if they have traffic.

- **Satellite Communications (SATCOM)**: In recent years the use of satellite transmissions has greatly assisted the Coast Guard in meeting their mission objectives. Commercial International Maritime Satellite (INMARSAT) and the government's Military Satellite (MILSAT) are the primary systems that the Coast Guard has employed.

  The Coast Guard recognizes that satellite system transmissions are the most reliable of the links that are available. It is the only transmission method that can reliably handle the high volume capacity involved in present-day ship-to-shore telecommunications. In response to this, the Coast Guard has installed tactical satellite equipment on board their appropriate vessels to support mission requirements.

  INMARSAT provides the Coast Guard with commercial voice and data telecommunications on a worldwide basis for both fixed and mobile platforms. Satellites providing worldwide coverage are in geosynchronous orbits at approximately 22,300 miles above the equator. Several satellites provide this service and have overlapping coverage footprints that extend across land and sea. Earth Stations provide complete communications coverage between ship and shore by linking mobile satellite users with international telephone, telex, and data networks.

The Coast Guard Data Network (CGDN) uses this technology to provide connectivity to mobile units.

The Coast Guard uses two types of INMARSAT terminals: INMARSAT A and INMARSAT C. INMARSAT A provides telephone, data (including e-mail), and telex services to larger vessels (typically over 45' vessels). It requires an antenna and a transceiver for above deck, and below it supports direct-dial telephones, telex machines, printers, facsimile, and modems. INMARSAT C is less expensive and is better suited for smaller vessels because both the electronics hardware footprints and antenna sizes are smaller. It is good for cost effective store-and-forward data messaging, position reporting, and remote monitoring. Coast Guard INMARSAT use has grown significantly in recent years.

Coast Guard assets have access to certain MILSATCOM systems based on unique operational requirements and interoperability needs with the U.S. Navy. The Navy UHF Fleet Satellite Communications (FLTSATCOM) system consists of leased satellites and portions of leased maritime satellites that provide world-wide communications connectivity with naval ships and airborne platforms. The FLTSATCOM system comprises space, earth, and control segments. Space and earth segments consist of satellites, earth terminals, subscribers, and subsystems. FLTSATCOM subsystems most commonly used by Coast Guard units are:

1) <u>Officer-in-Tactical Command Information Exchange Sub-system (OTCIXS)</u> which provides a two-way link to support inter- and intra-battle group over-the-horizon targeting tactical command and control data communications in a near-real-time (1-15 minutes) environment. It provides a gateway to the SIPRNET which allows bi-directional tactical data links between shore commands and OTCIXS equipped units. OTCIXS is currently used by 378s and 270s, and is being installed on 210s and Transportable Communications Centers (TCCs).

2) <u>Common User Digital Information Exchange Subsystem (CUDIXS)/Naval Modular Automated Communications Sub-system (NAVMACS)</u> provides a 2400 baud full duplex interface over a satellite link with mobile platforms. NAVMACS provides up to four channels of fleet broadcast input, a subscriber interface to CUDIXS and other on-line message functionality. NAVMACS on Coast Guard cutters is configured with Coast Guard Standard Workstation (CGSW) equipment and supported by the Shipboard Telecommunications Computer System (STCS).

3) <u>UHF Demand Assign Multi-Access (DAMA) Sub-system</u> provides users with increased communications capacity and reliability over dedicated access on the FLTSATCOM satellites. DAMA is capable of multiplexing secure voice, record message, and data sub-systems onto a single 24 kHz satellite channel.

WAGBs, WHECs, and 270s have DAMA, while 210s and the TCCs are being upgraded.

- Search and Rescue Satellite System (SARSAT) monitors distress alerts from 212.5 MHz and 406 MHz emergency position-indicating radio beacons (EPIRB), and transmits data to the NOAA Mission Control Center operating the U.S. portion of the COSPAS SARSAT system.

2.2.2.2 Landlines

Landline systems apply to communications transmission systems that are fixed, land-based, extremely reliable and somewhat permanent. The Coast Guard can extend landline systems to underway vessels and aircraft via radio systems, microwave, and satellite systems. The following are several of the shore network landlines that the Coast Guard uses to support their mission requirements.

- **Coast Guard Data Network (CGDN)**: The CGDN is the primary means for non-secure (clear) Coast Guard shore-side data communications. Its use is mandated by Commandant policy. CGDN connects virtually every shore facility and many major cutters in their home ports.

  The CGDN has evolved over time. It currently uses the X.25 protocol switches (proprietary TP line) of FTS2000. The backbone consists of switching nodes located at each continental United States (CONUS) District Office, Operations Systems Center (OSC), and Coast Guard Headquarters. The network contains redundant links to maintain a high level of reliability by ensuring continuous connectivity. Should one of the backbone circuits suffer a catastrophic failure, there is another path to sustain the telecommunications between nodes.

  Some of the major applications that ride the CGDN include the Marine Safety Information System (MSIS), Law Enforcement Information System (LEIS), Personnel Management Information System (PMIS), and e-mail. E-mail is extremely important because many applications use e-mail envelopes to transmit application specific information from point to point. The CGDN uses e-mail as the transport mechanism to support file transfer in applications such as the Large Unit Financial System (LUFS) and PMIS.

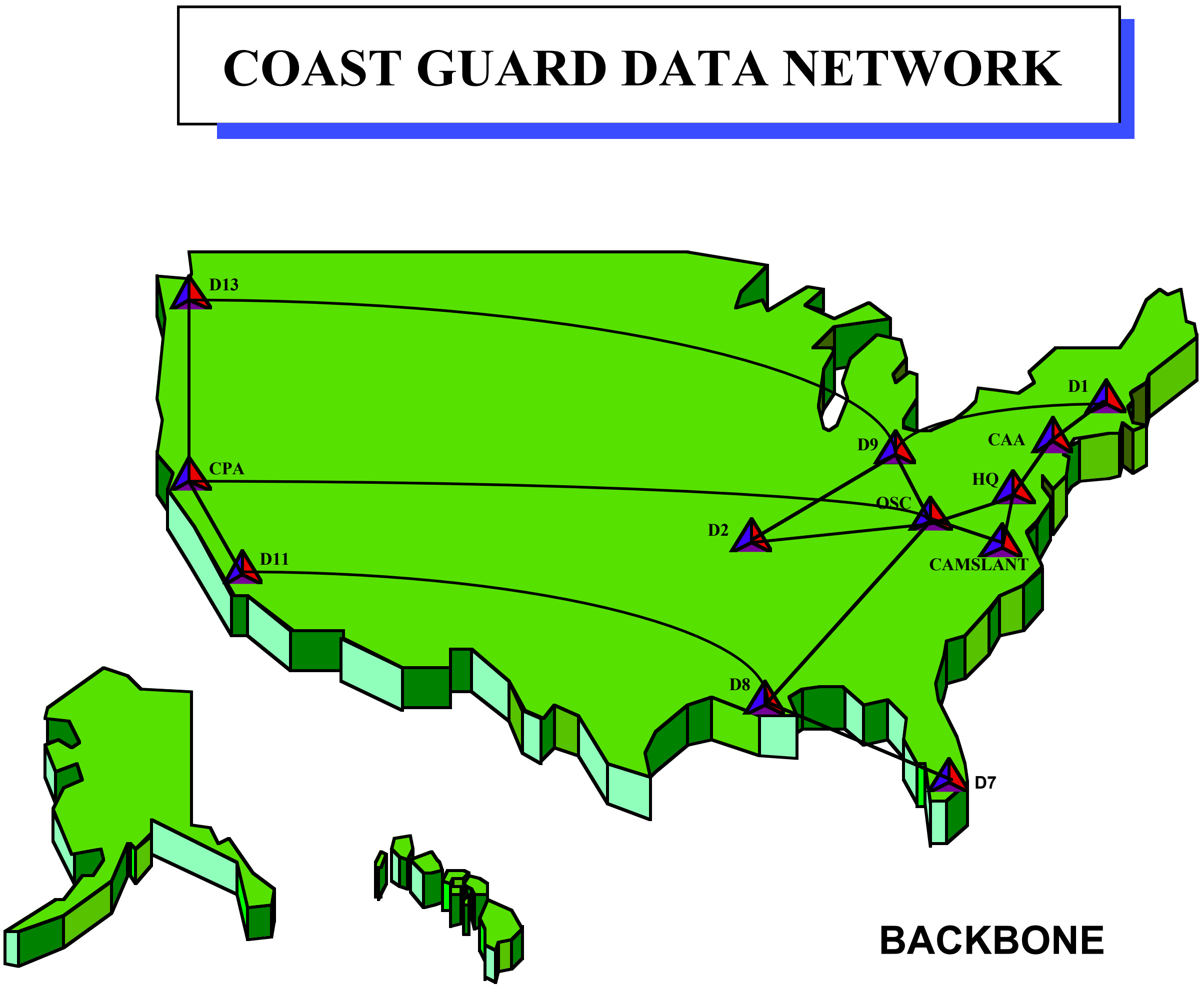


Figure 2-1: Coast Guard Data Network (CGDN)

Tail circuits, connected via typical star configuration, from each of the above CGDN backbone nodes, expand and extend the CGDN down to various types of users in CONUS, Alaska, and Hawaii. These include Group Offices, Air Stations, MSOs, and Support Centers. Tail circuits are required to meet command and control, administration, and maritime public support requirements.

- **Standard Semi-Automated Message Processing System (SSAMPS)**: SSAMPS consists of CGSW-II hardware and Coast Guard developed software and is installed at each of the Coast Guard COMMCENs and COMMSTAs. It performs all of the actions necessary to route incoming/outgoing messages to their addressee(s), including selecting the proper circuit. The software directs the flow of messages based on Plain Language Addresses (PLAs). In addition, it maintains a complete system transaction log.

- **Automatic Digital Network (AUTODIN)**: AUTODIN is a secure, world-wide Defense Communications System (DCS) store and forward network that serves as the

Coast Guard's primary secure record message system. It does this by providing the bulk of inter-district and inter-agency telecommunication connectivity for record message traffic.

The Naval Communications Processing and Routing System (NAVCOMPARS) provides the interface between shore networks, and provides automatic message processing, formatting, and conversion.

Table 2-1: Coast Guard AUTODIN Connectivity

- **Secure Data Network (SDN)**: The SDN provides a dial-up secure, low volume record message capability extending from Districts down to Groups, Air Stations, MSOs, selected COMMSTAs, and other units.

- **Teletypewriter Exchange Network (TELEX/TWX)**: The Coast Guard leases services from commercial telegraph companies to provide rapid teletypewriter communications with the commercial sector. TELEX/TWX allows them to communicate with other non-Coast Guard subscribers through direct dialing services.

- **Imagery and Facsimile (FAX)**: Imagery applies to the transmission and reception of images that include, but are not limited to photographs, drawings, forms, and other graphical data. FAX applies to the transmission and receipt of unclassified and classified information, up to and including Secret using current international facsimile standards. Ice and weather facsimile broadcasts are made by designated Coast Guard COMMSTAs.

- **World-Wide Military Command and Control System (WWMCCS)**: WWMCCS allows National Command Authorities and the National Military Command Center to exercise command and control of their forces. This command and control extends down to the level of the supporting command.

  WWMCCS also provides the necessary support for the Joint Operations Planning System and extends to Automatic Data Processing (ADP) facilities who support joint operations.

  WWMCCS is being replaced by the Global Command and Control System (GCCS) which will be fully interoperable with existing afloat and ashore command systems to provide a common operating environment for all. Coast Guard users will be

Headquarters and Area command centers. GCCS provides the same chart display, track management, and tactical data link capabilities as WWMCCS.

- **Secret Internet Protocol Router Network (SIPRNET):** SIPRNET is a wide-area network (WAN) consisting of a collection of backbone routers interconnected by high-speed serial links. It is used for passing datagrams, at the Secret-Not Releasable to Foreign Nationals (SECRET-NOFORN) classification level, to subscribers within DoD and other government agencies. The network supports data traffic, but will eventually also support voice and video services.

- **Anti-Drug Network (ADNET):** ADNET allows DoD counterdrug and law enforcement agency users to access and share information from a variety of DoD and law enforcement agency sensor/surveillance resources through the rapid transfer of graphics, text, and contact data classified to the SECRET level.

2.2.3 Video

We have broadly divided video teleconferencing into three general categories: Satellite-based broadcast video teleconferencing, desktop video teleconferencing, and group (large or small) video teleconferencing. Each type has an optimal application. For example, satellite broadcast video teleconferencing is ideal for training in which a single speaker wishes to reach a large number of remote sites simultaneously for a low cost. Group video teleconferencing is ideal for two geographically separated groups to work together, using two-way video and graphics sharing.

Video teleconferencing offers the potential to significantly reduce travel costs and increase productivity. It is a tool which can greatly improve the work processes between units by offering quick, affordable, and efficient communications. Reductions in travel costs alone will justify the installation of video teleconferencing systems in many locations.

2.3 Baseline Architecture

The following diagrams show a high level view of the telecommunications infrastructure, including incoming and outgoing circuits and systems.

2.3.1 Communication Centers (COMMCENs)

The COMMCEN diagram was developed from visits to the LANTAREA/D5 and PACAREA/D11 COMMCENs. The consolidated these COMMCENs as a result of Streamlining. Each of the remaining district staffs and Coast Guard Headquarters are served by its own COMMCEN. Networks connect these COMMCENs to communications facilities and other operational and administrative commands. COMMCENs provide access to the commercial and secure military common user networks through which the bulk of the interservice message traffic flows.

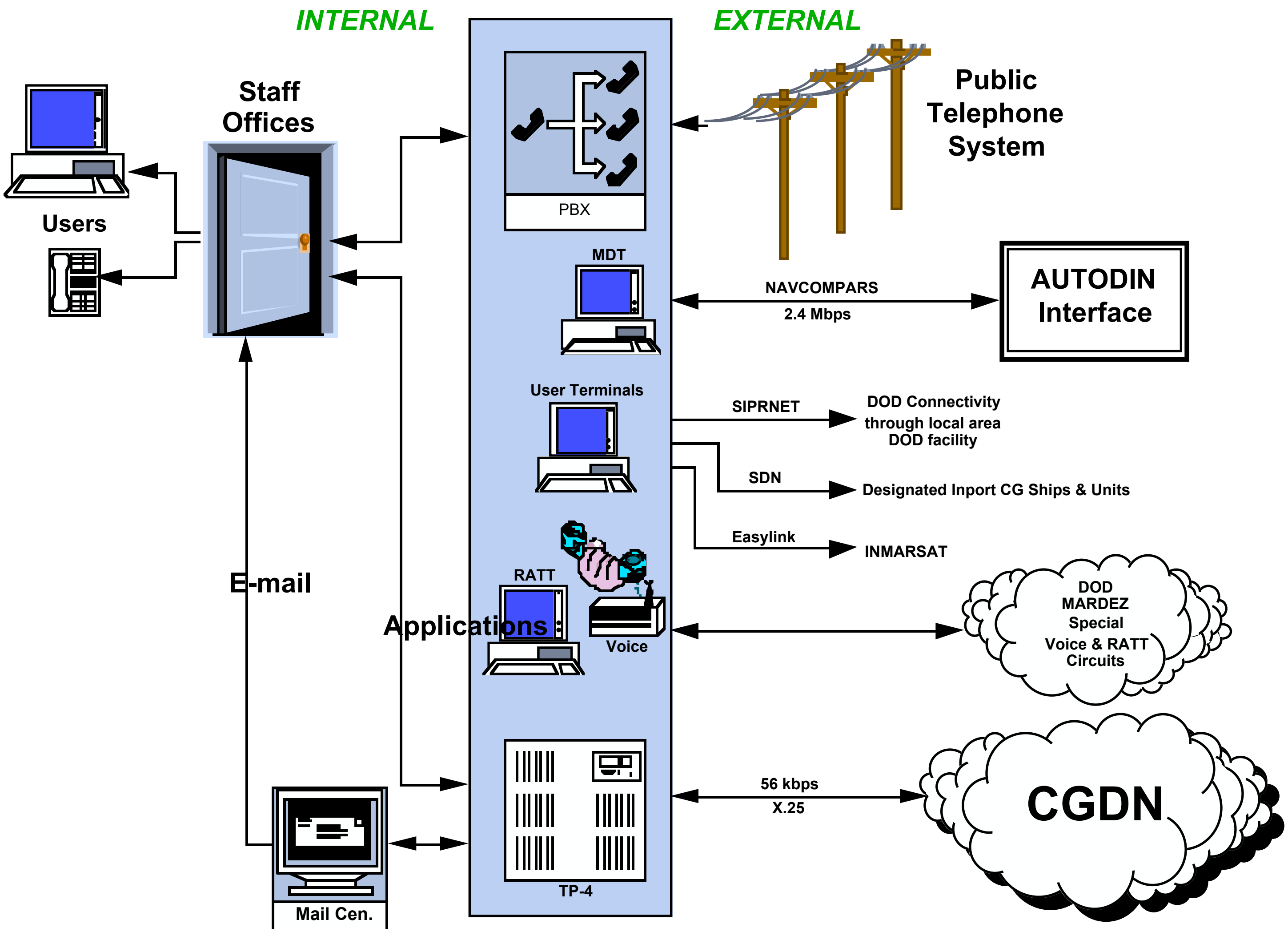
Commercial networks, such as the public telephone system and Easylink, are routed through the COMMCENs. Users access the telephone system for standard voice communications and in some applications require direct dial-up modem capability. Easylink provides access to the commercial INMARSAT system.

COMMCENs provide nodes in the following military systems: CGDN, AUTODIN, SIPRNET, and SDN. CGDN uses the COMMCENs as nodes along the system backbone and they are usually the routing point for several smaller capacity tail circuits to various administrative and operational units. The COMMCEN provides the gateway into CGDN for the LANs serving the district/area/HQ staffs. The users communicate via e-mail service-wide and with external entities through the LAN and CGDN. Application programs may also take the same route. In many cases the applications use e-mail envelopes to transmit data over the LAN and CGDN. AUTODIN hook-ups provide access to the Navy's record message system. Electronic delivery of messages over the LAN to the desktop is the currently accepted approach. Users access ADNET, JMIE, and other intelligence systems over the covered DoD network called SIPRNET. The COMMCENs use SDN to provide classified message service to low-volume users via a dial-up connection and STU-III telephone.

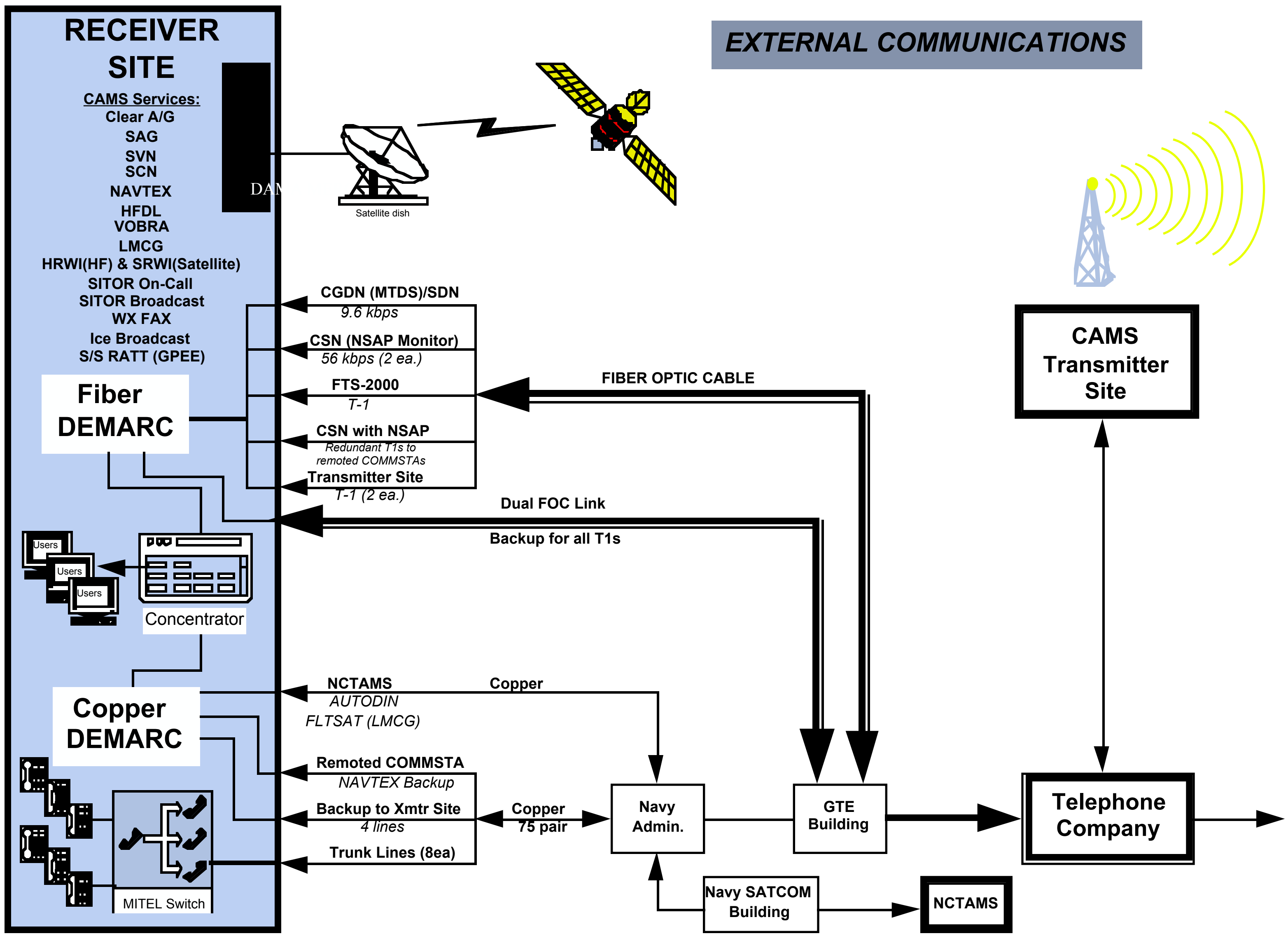
Some (but not all) COMMCENs have DoD special circuits for voice and RATT support of Maritime Defense Zone (MARDEZ) operations. Some provide tactical voice services (i.e. D7) while others may use civil defense radio frequencies or limited maritime mobile communications (VHF-FM) (this is mainly provided at the group level and below.)

Most district COMMCENs maintain a one person, 24 (hours) by 7 (days) watch to monitor communications networks, circuits and systems. This network control center process has evolved to become the primary purpose of the COMMCENs. During peak loading times this watch must be augmented. COMMCENs (Areas and HQ) with greater communication volumes and numbers of equipment require multi-person watches.

Communication Center (COMMCEN)



COMMSTA Telecommunications System



2.3.2 Communication Stations (COMMSTAs)

We have modeled the above diagram after Communication Area Master Station Atlantic (CAMSLANT). It represents a typical Coast Guard Communication Station (COMMSTA). The diagram provides a high level overview of the communication services and operational circuits currently in use at CAMSLANT. All Coast Guard COMMSTAs perform all or some portion of these functions. However, individual COMMSTAs may have certain unique requirements that are not shown in this diagram.

The mission of a Coast Guard COMMSTA is to provide rapid, reliable, and secure communications support and services to Coast Guard operational commanders, other government agencies, and military and civilian organizations throughout the world. The CAMS coordinates day-to-day Communication System (COMMSYS) operations as well as provides administrative and technical oversight of individual stations within the system. The CAMS coordinates broadcast operations and loading conditions, and ensures efficient communications workload distribution throughout the COMMSYS. They also provide for the reallocation of communications assets during planned outages, communication casualties, or minimize, and provide current system user information via COMMSYS message directives. As the "supervisor" of the COMMSYS, the CAMS approves requests from COMMSTAs for planned communication outages, and uses available frequency propagation software to make frequency predictions when necessary. And, among many other duties, they ensure prompt response to reports of communications problems, resolve disputes incident to message handling within the COMMSYS, establish and operate a communication drill and exercise program, coordinate a quality control monitoring program, and maintain an active COMMSYS ship contact program providing for exchange of system information.

COMMSTAs provide several around-the-clock communications services to the Coast Guard fleet, Navy vessels, and the maritime public. These mission essential operations include clear and secure ship-to-shore voice and radio teletype circuits; clear and secure air-to-ground circuits; broadcast services, including VOBRA where broadcasts are made automatically using computerized voice transmissions; and various data transmission services, such as NAVTEX, SITOR, and HFDL.

2.3.3 Group Offices

The Group Office COMMCEN provides rapid and reliable voice and data telecommunications support to meet Group operational requirements, such as SAR, Law Enforcement, and Aids to Navigation (AtoN). They also provide messaging services in support of Group administration and supply. In addition, the Group COMMCEN provides all data and Communications Security (COMSEC) support to units (stations, aids-to-navigation teams, and cutters) under their control. Some Groups also maintain the radio guard for their local Marine Safety Office mobile units.

Coast Guard Groups normally transmit and receive unclassified record message traffic via CGDN. They send and receive classified message traffic by other means, such as the SDN or over-the-counter message service from the District Office or other major unit. E-mail and several

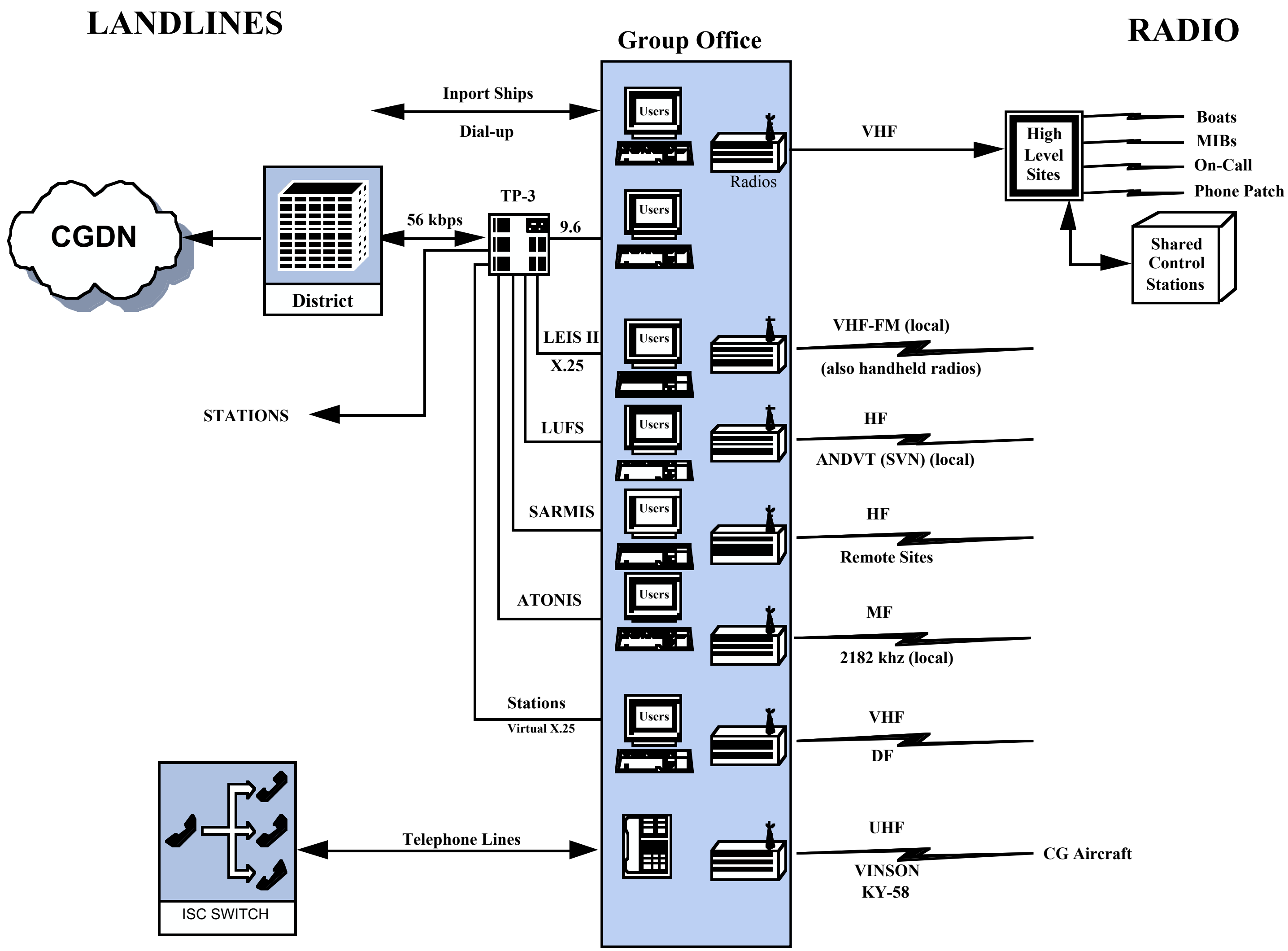
Mission Essential Applications (MEAs), such as ATONIS, LEIS-II, LUFS, and SARMIS, also use the CGDN to connect with the end-user or servicing computer system.

All Groups have VHF-FM capabilities, which normally consists of a Channel-16 guard receiver, and transmit and receive capabilities on Channel-16 and several local area working frequencies. Some may also have MF capabilities for meeting coastal maritime public communications requirements (i.e. SAR and notices to mariners), and HF for working aircraft and long distance vessel communications. Some Groups have dual VHF-FM suites of equipment in their radio console. This provides redundancy for their VHF-FM operations, where one is the backup for the other. Most Groups have remote VHF-FM transmitters and receivers located on towers, constructed on high ground or buildings in select locations (High Sites). These sites help them reach the limits of their area of responsibility with a high degree of reliability.

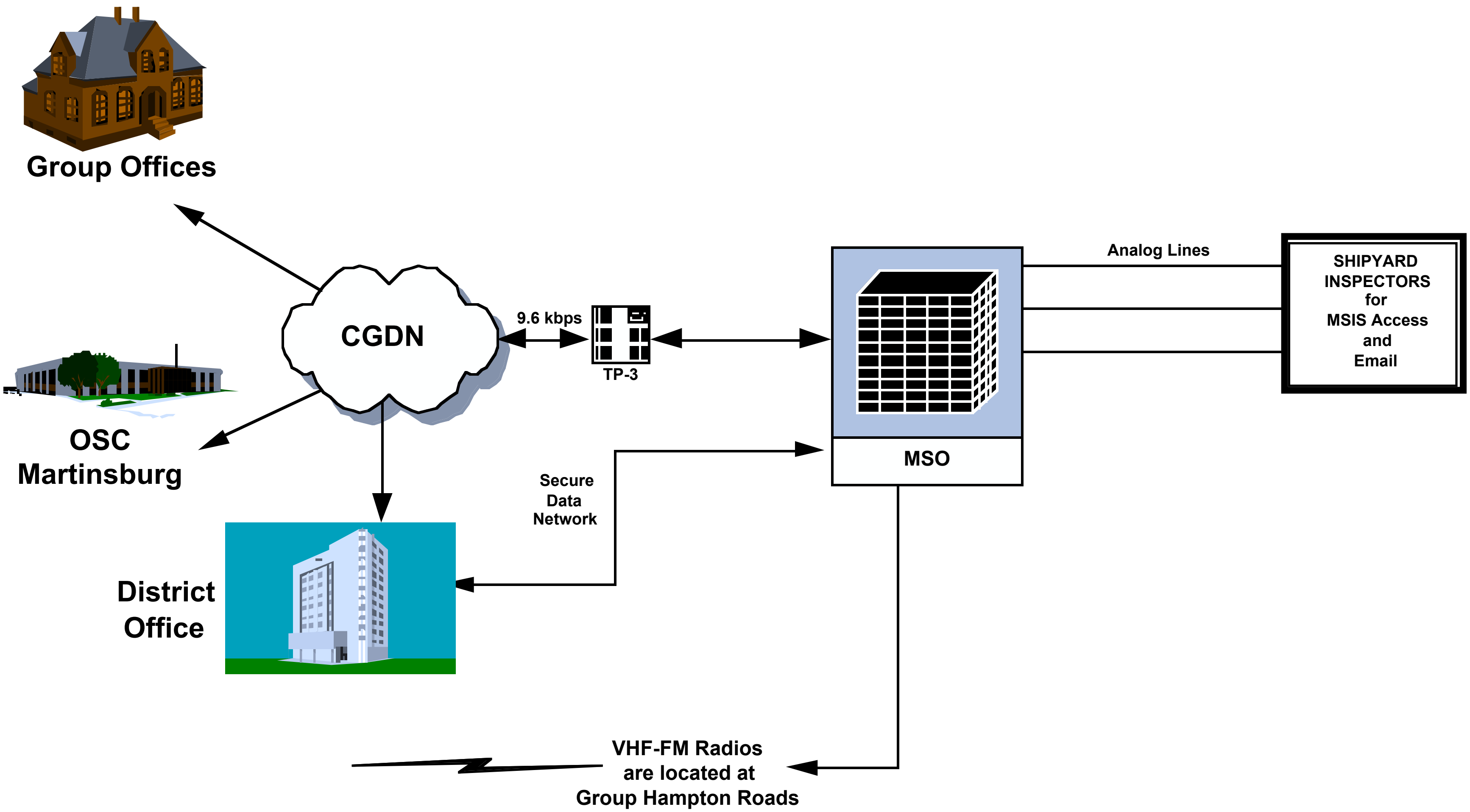
In the radio console, most Groups have a quick access recording tape (approximately 30 minutes of recording time) for monitoring radio transmissions. This provides the radio operators with the ability to go back and listen to recent radio transmissions when necessary.

To meet message traffic workload and radio guard requirements, some Groups maintain a two person watch, 24-hours a day. However, most Groups require only one watchstander, under normal conditions, with additional personnel supplementing the watch during peak periods.

Group Office Telecommunication System



Marine Safety Office Telecommunication System



2.3.4 Marine Safety Offices

The Marine Safety Office is the unit under which field unit functions of the entire Marine Safety Program (Commercial Vessel Safety, Marine Environmental Protection, and Port Safety and Security) are consolidated. The Commanding Officers of these units have responsibilities of Officer-in-Charge of Marine Inspection, Captain of the Port, and are the predesignated Federal On-Scene Coordinator (FOSC) for maritime spills within their Area of Responsibility (AOR). There are several Marine Safety Detachment (MSDs) which are smaller versions of their parent commands.

The most pressing need for communication at the MSOs/MSDs are data lines for connection to MSIS. This interactive, vessel -oriented, real-time database is described in section 2.7 under Marine Safety Network (MSN). Normal MSO connection to MSIS is through a local phone switch into the Coast Guard Data Network. As CGDN users, MSIS operators use CGSWs II and an X.25 protocol to access the OSC Martinsburg based application. Units in more isolated areas (usually MSDs) and detached shipyard inspectors rely on dial-in modems to access MSIS. MSIS access is extremely important to the Marine Safety community where around-the-clock, real-time access is necessary to conduct many MSO operations.

Another busy application at Marine Safety field units is e-mail. This allows rapid and relatively informal message communication with nearly every other terminal within the Coast Guard.

Depending on unit missions, MSOs may have VHF-FM radio capability. That may be an antenna on the MSO building roof or a shared capability with a Coast Guard Group or Air Station.

Most MSOs have a Secure Data Network capability for the occasional classified message.

MSOs have infrequent but pressing needs for additional communications support during contingency operations. Most often the precipitating event will be an oil spill of large proportion. These operations are people, data, and communications intensive. Support is available from the local district and may come from Coast Guard Headquarters if required. The telecommunications demands are usually for portable communications, computer resources, and telephone augmentation. All these are required to equip a situation command center.

2.3.5 Air Stations

The diagram below is modeled after one Coast Guard Air Station’s telecommunication system. Other Coast Guard Air Stations may have unique telecommunications systems or equipment not shown in this diagram.

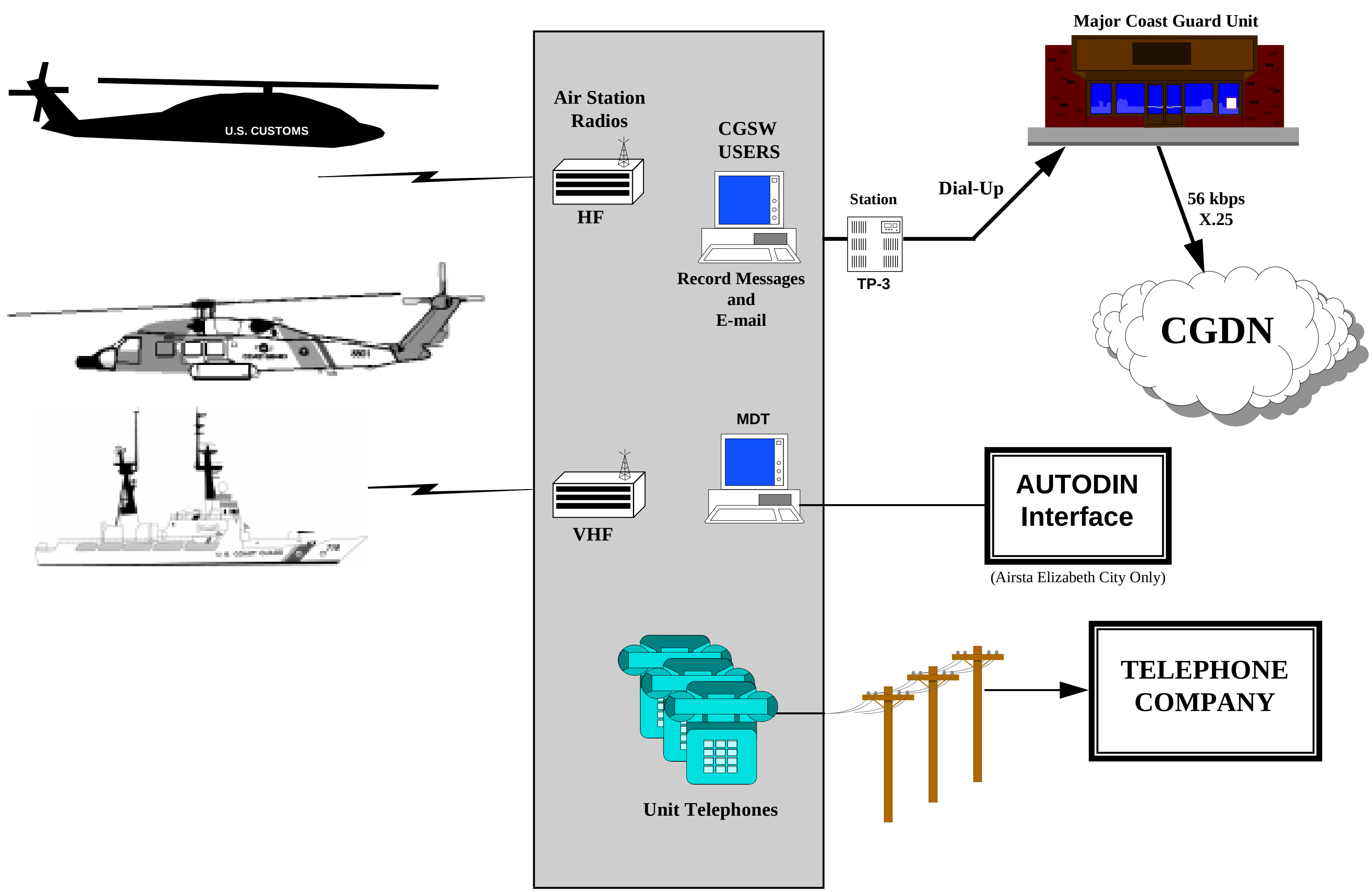
The primary function of the Air Station COMMCEN is to provide rapid, reliable, and secure telecommunications support and services around-the-clock for unit operations and administration.

Air Station Elizabeth City, North Carolina sends and receives unclassified and classified record message traffic via AUTODIN using a Message Distribution Terminal (MDT) connection. Other Air Stations use a combination of CGDN (unclassified) and SDN (classified).

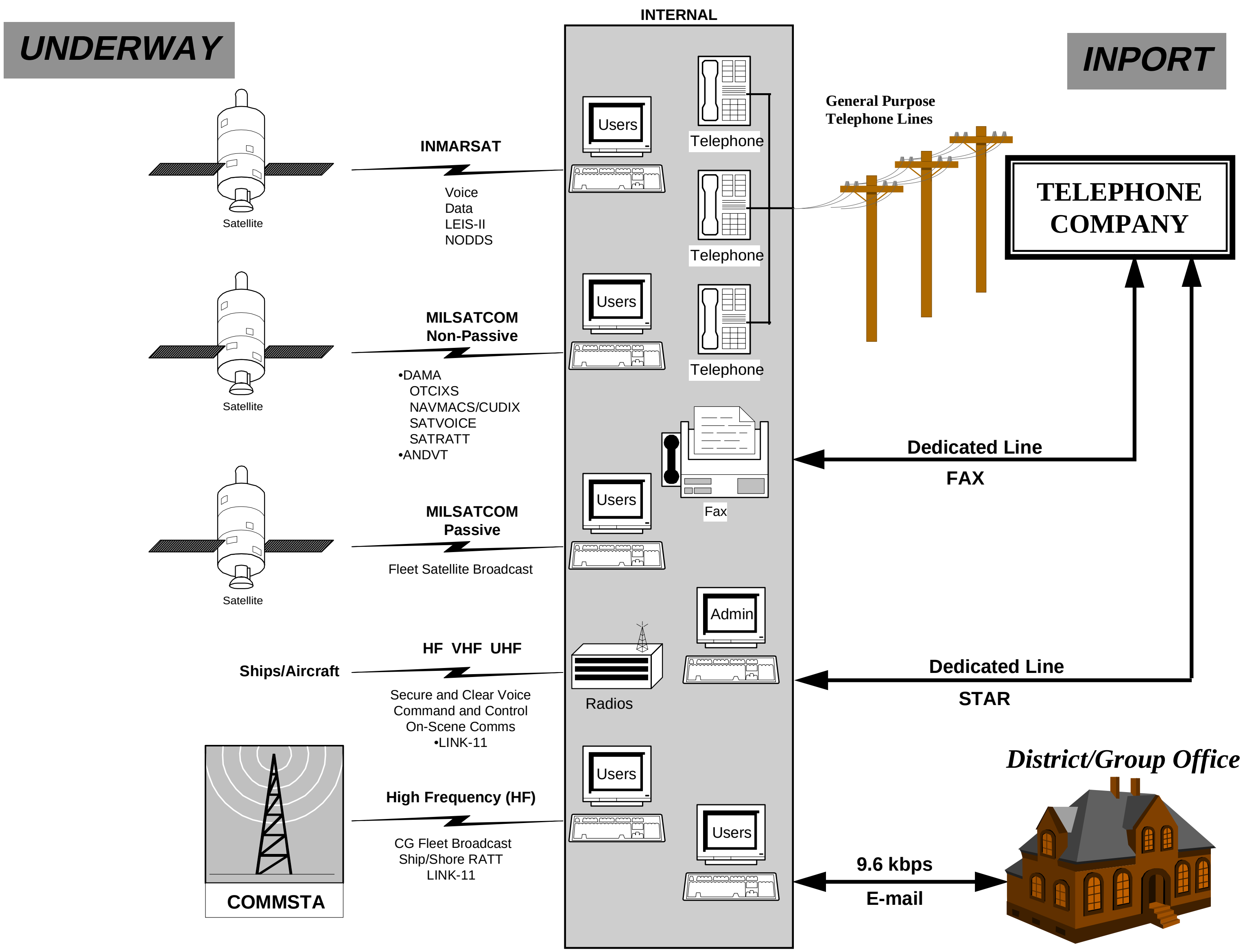
CGDN is used for sending and receiving record message traffic and e-mail, and also for applications, such as STAR and AMMIS.

Many air stations require radio communications to meet their day-to-day operations and crisis management needs. They have varying requirements for connectivity and interoperability with local regional Federal agencies (e.g. DoD, FBI, DEA, Customs, etc.), state and local government agencies and the general public, and with fixed and mobile Coast Guard platforms, including underway Coast Guard vessels and aircraft.

Air Station Telecommunication System



WHEC/WMEC Telecommunication System



2.3.6 High/Medium Endurance Cutters (WHECs/WMECs)

While in port, WHECs and WMECs connect to various systems through telephone lines. A typical WHEC or WMEC may have one fax line, one modem line, and four telephone lines. These lines provide regular telephone services for voice and data transfer applications, such as LUFS and STAR (replacement for ARMS). Ships do not generally have direct access to CGDN. The ShipNet project is making those connections, but is not yet widespread. They use the modem connection to attain CGDN access from an available shoreside Coast Guard command. This gives them e-mail capability. They usually dial up through the same command to access SDN for transfer of classified traffic via STU-III. Unclassified message traffic, is received via the email link and distributed, in most cases, electronically by Message Board software. The Message Preparation and Review Software (MPRS) is available to ships, but is not in wide use as yet.

While underway, they process record message traffic via satellite circuits using CUDIX—dropped calls are not common for this system. Classified and unclassified messages are split as they arrive. They normally average 100-150 messages per day (350/day during high tempo operational periods). HF RATT is used for copying the Coast Guard FRTT (Fleet Broadcast) and for FULL TERM operations with a COMMSTA. OTAT (Over-The-Air-Transfer) updates crypto keying material while underway.

An AN/UYK-20 computer serves as the backside to CUDIX which takes traffic, presents screens, and distributes information. They have an CGSW-II that acts as their Cluster Communication Workstation. Status of Resource and Training System (SORTS) information is transferred via satellite through CUDIX. Other communications equipment that may be on board: UHF DAMA capable WSC-3, WSC Patch Panel, Access to Link 14, OTCIXS, AN-WSC-3(V), and KYV-5’s (UHF, Satellite (INMARSAT)). They access Satellite Radio Teletype (SATRATT) via Military Satellite (MILSAT).

Most of the ship’s voice traffic is handled in the Combat Information Center (CIC) where they have a secure MILSAT voice switchboard. Voice communications include VHF, UHF, and HF (clear and secure Advanced Narrowband Digital Voice Terminal (ANDVT)), and INMARSAT. Many have INMARSAT-C, which is used to access the LEIS-II database.

OTCIXS, along with JMCIS (Joint Maritime Command Information System), is used for video display of operational information.

2.3.7 Buoy Tenders

The primary mission of Coast Guard buoy tenders is to provide support to the aids to navigation program. However, buoy tenders also provide support, on occasion, to Coast Guard law enforcement and drug interdiction efforts, and also respond, as needed, to search and rescue, and marine environmental protection calls.

While in port, telephone systems provide the primary means of external communications. Ship telephones are compatible with commercial telephone systems. Telephone lines are also used for modem (X.25) connection to the CGDN, for sending and receiving record message traffic and e-mail, and for Mission Essential Applications (MEAs), such as AIMS, STAR, LEIS-II. Classified messages are usually delivered to the cutter via over-the-counter service from a local Group Office or other major Coast Guard/DoD unit.

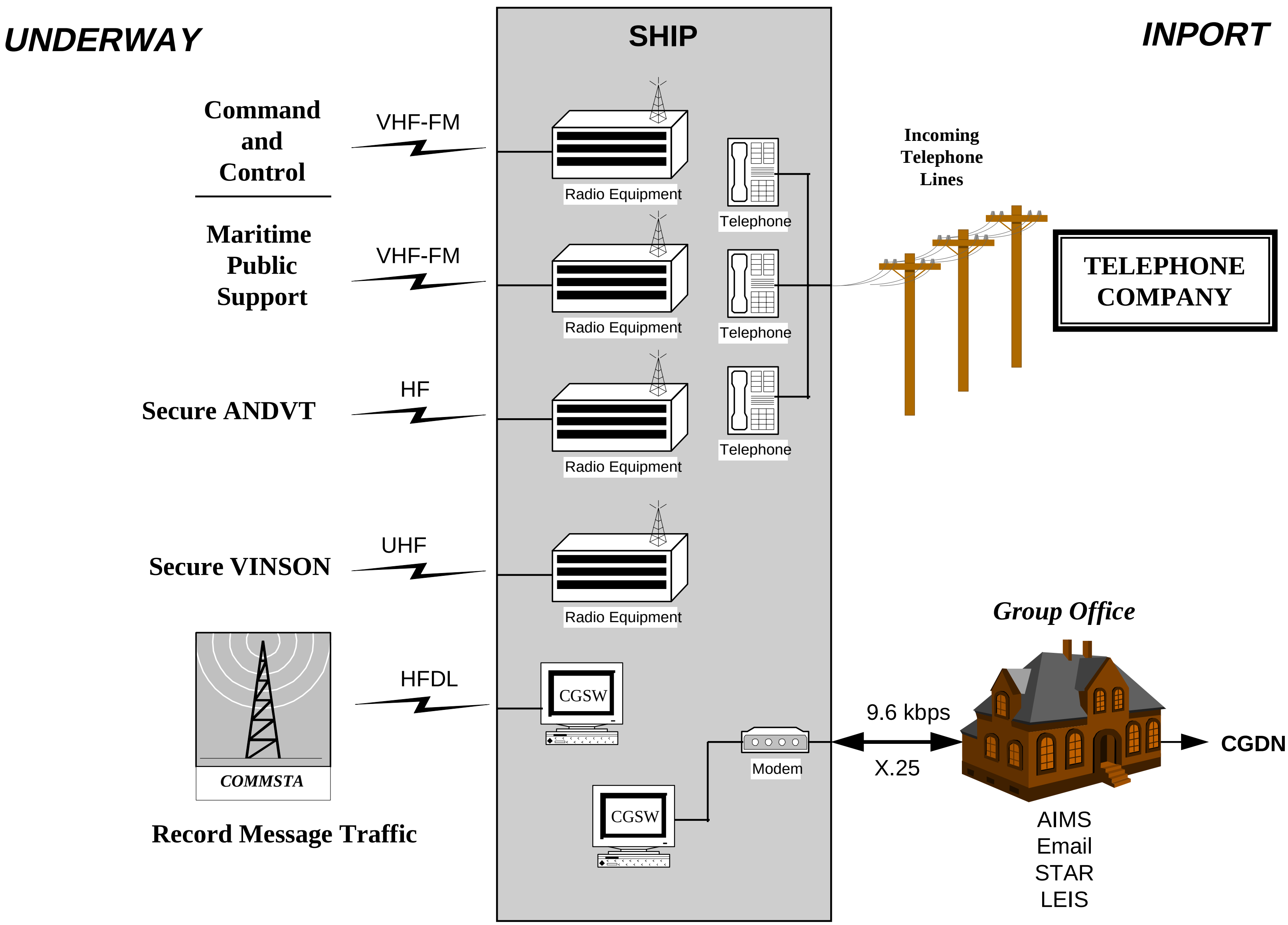
Conversely, radio systems become the primary means of external communications while underway. These systems include VHF-FM, UHF, and HF, on which the ship communicates with Coast Guard units, other government agencies, and the maritime public.

VHF-FM is used primarily for short distance (line of sight) on-scene command and control, and is often used to work voice traffic with other government agencies and the maritime public. Buoy tenders may have several VHF transceivers for communications on various VHF-FM channels (e.g. 16, 13, 21A, and 14).

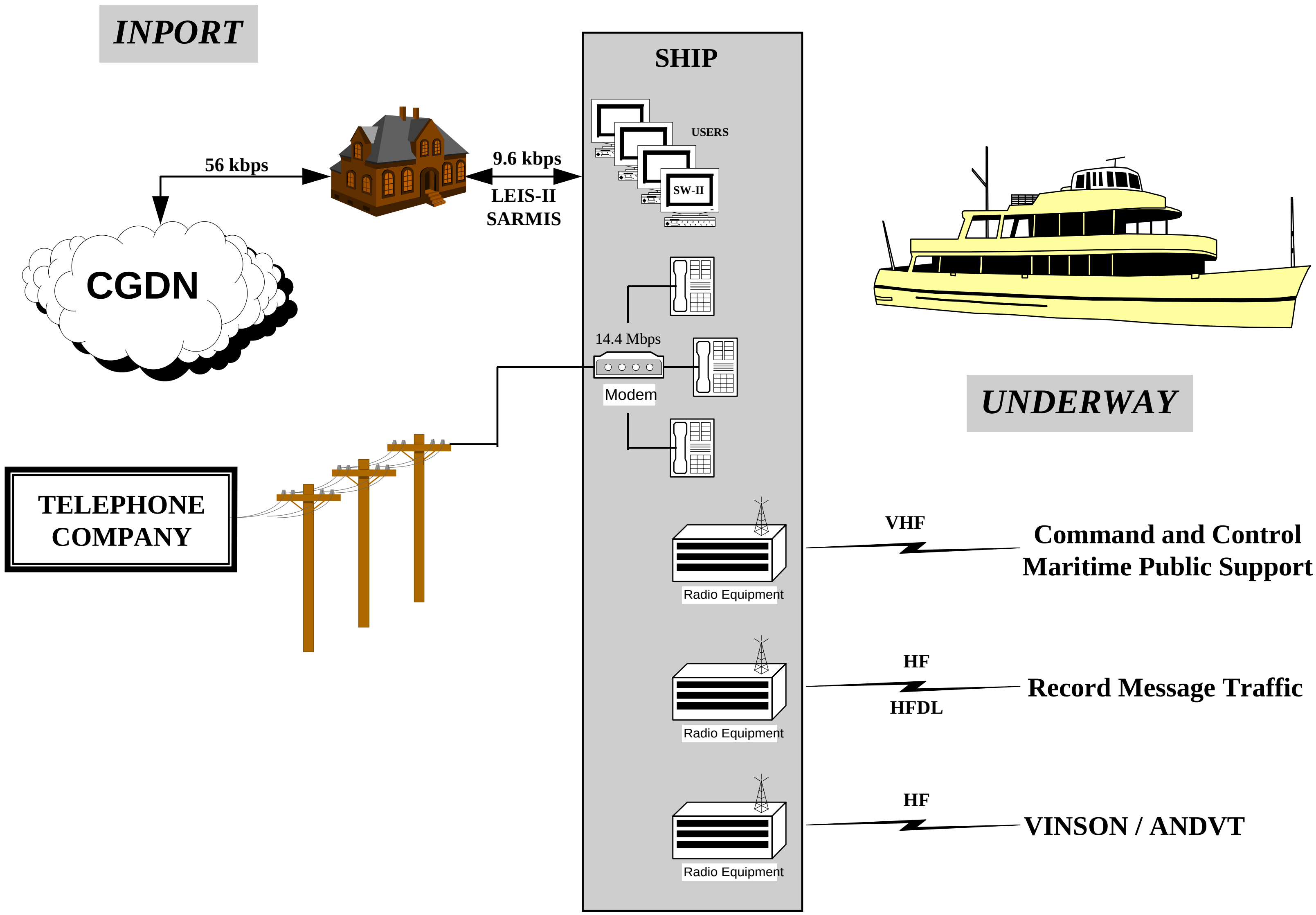
GSB-900 HF transmitters are used for clear and secure (ANDVT) HF voice (for working long distance communications with vessels and aircraft) and HFDL (record message traffic) communications with a COMMSTA. The Coast Guard normally uses HF only on extended voyages where the ship is not returning to their home port each night.

The Coast Guard uses UHF for short distance (line of sight) secure (VINSON) on-scene communications with other ships and aircraft.

WLB Telecommunication System



WPB Telecommunication System



2.3.8 Patrol Boats (WPBs)

While shoreside, WPBs electronically access e-mail through a physical 9.6 kbps connection that links them to their Group, which in turn connects them to the CGDN. Several telephone lines are connected to the boat for voice telephones, a dedicated data line for applications, such as LEIS-II and SARMIS, and also a 14.4 baud modem line.

Underway, they send voice message traffic via VHF-FM through the closest Group Office or via HF with CAMSLANT/COMMSTA. HFDL is used for sending record message traffic while underway on extended voyages. They can also communicate with a COMMSTA in a secure mode, on HF, using ANDVT.

In addition, they appropriately disperse e-mail messages electronically or by paper copy. They bring up message traffic using SSAMPS. They have approximately three CGSW-II terminals for administration, supply, and operations, and an HFDL terminal for sending and receiving record message traffic. They rely on the Group as a router—their email gets relayed to the Group and they retrieve it in port via dial-up access.

They have limited long and short range communications capability. They typically have a GSB900 HF system and two MCX 1000’s (one MCX guards the distress frequency and one MCX guards working frequency). They have ANDVT Red Phone (green and red switching) and a VINSON Red Phone. They may also have cellular telephone capabilities.

2.3.9 Small Boat Stations

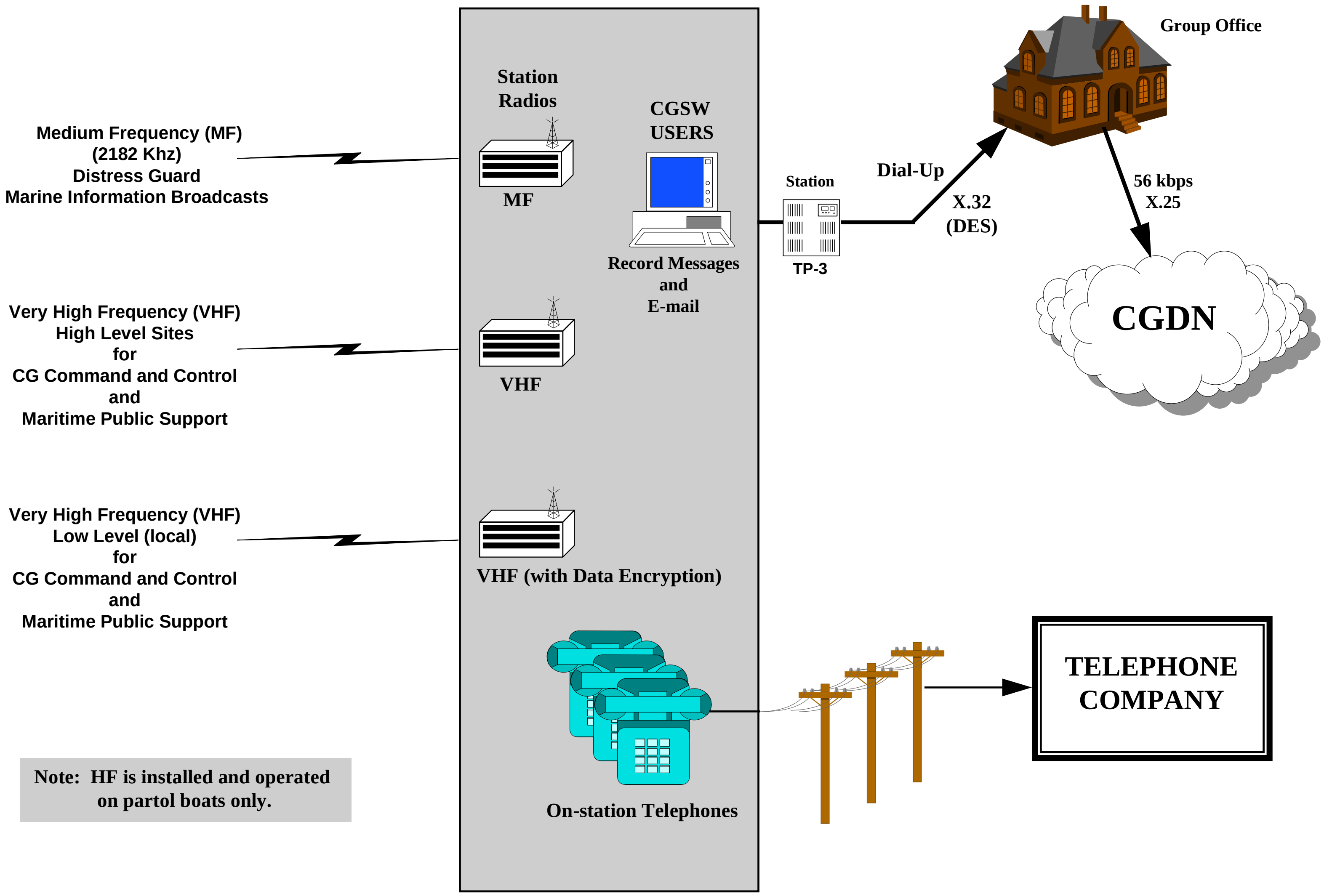
Small Boat Station communications capabilities are very similar to those of the Group Office. As a minimum, shore stations with assigned SAR duties possess a send/receive VHF-FM voice capability and a guard receiver for the primary distress frequency. They often act as the alternate control for the national VHF-FM and/or coastal MF High Sites. A data link with the Group, portable and vehicular radios, and commercial and FTS telephone service are also provided where required.

VHF-FM is used for Coast Guard command and control, and for maritime public support. With transmit and receive capabilities both locally (low level) and through access to the Group High Level sites, Stations can effectively provide customers with reliable communications coverage to the outer limits of their operating area.

Coast Guard small boat stations use MF for distress, marine weather and safety broadcasts, and other maritime safety purposes. Nominal coverage provided by Coast Guard MF systems is approximately 200 NM offshore.

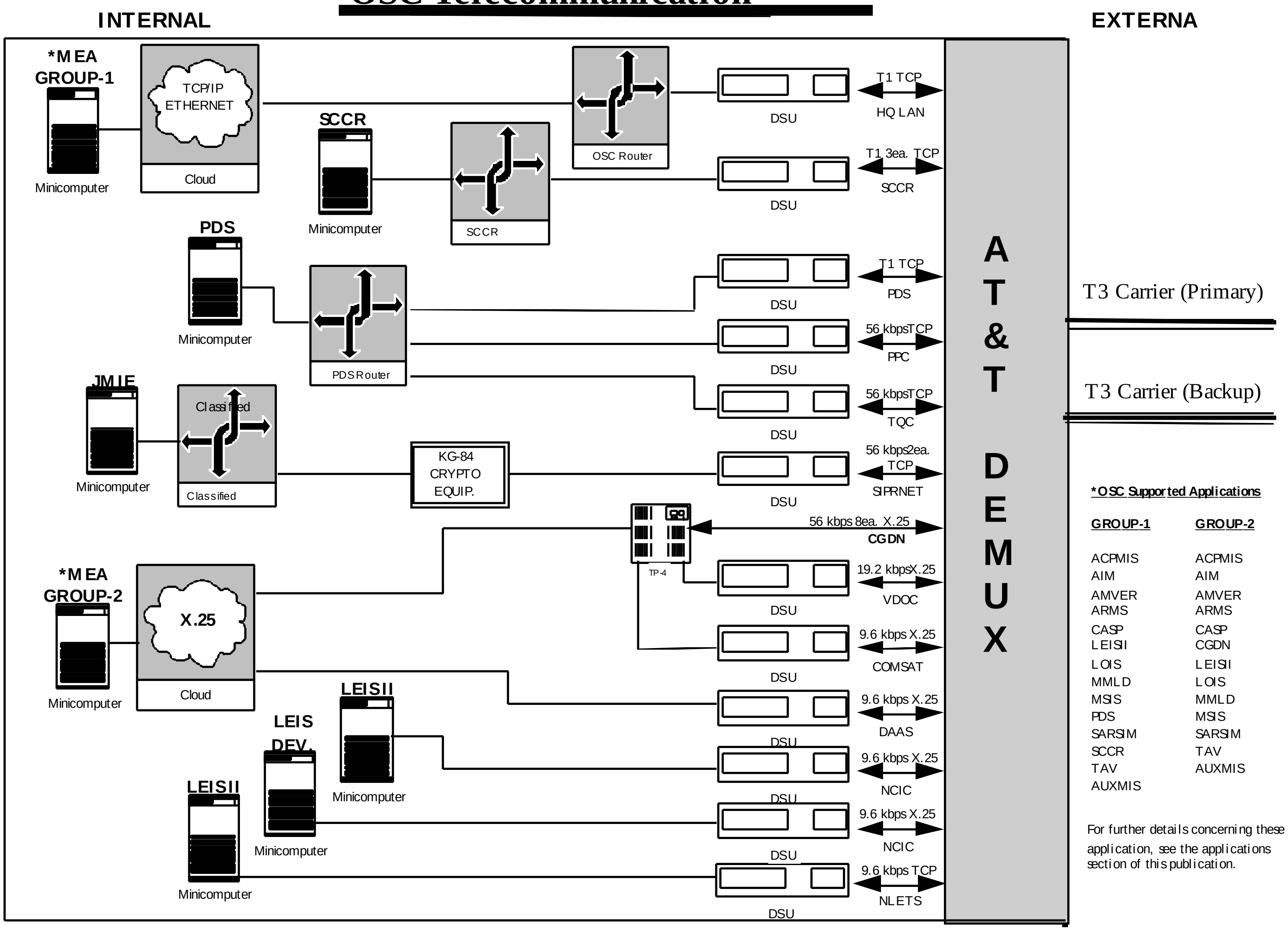
A dial-up, Data Encryption Standard (DES) protected connection, to the Group’s TP-3, is used to link to the Station to the CGDN. Record message traffic and e-mail messages are sent and received over this circuit.

Station Telecommunication System



Note: HF is installed and operated on partol boats only.

OSC Telecommunication



2.4 OSC Martinsburg

OSC develops, fields, maintains, and provides user support for major operationally focused information systems and data bases that are accessible to the Coast Guard around-the-clock from around the world. These systems serve as the information heart of the Coast Guard's SAR, law enforcement, marine safety, and logistics support functions. OSC also serves as the network control center for the Coast Guard's wide area data network and carries out the Automated Information System risk analysis program for other data centers and major mission critical software development projects.

The OSC was designed and constructed to be a state-of-the-art computer support facility able to accommodate additional systems to meet the Information Resource Management (IRM) needs of the Coast Guard. With the advent of Government open systems standards, the OSC was also designed for sharing of system resources among many applications for maximizing flexibility and minimizing costs, both recurring and nonrecurring, and for implementing and supporting those systems.

Prime computers (6-12 MIPS ea.) provide support for mission critical applications, such as AMVER, MSIS, LEIS, and CASP. A TP-5, which is linked to a TP-4 in the COMMCEN, is used for the CGDN. Other MEAs (e.g. LEIS-II, PDS, SARSIM, etc.) run on various OSC mini-computers.

OSC maintains a 24-hour operation where several telecommunications circuits, including EasyLink, CGDN, and secure FAX provide messaging service for OSC operations and administration. They use SSAMPS with the new MPRS to processing record message traffic to the desktop. Their equipment suite includes CGSWs, crypto equipment, and a TP-4 telephone switch. In addition to processing message traffic, they monitor several circuits, with emphasis on AMVER messages where they watch closely for requests for Search and Rescue assistance. They will soon be going to broadband TCP/IP.

2.5 Supply Center Curtis Bay (SCCB)

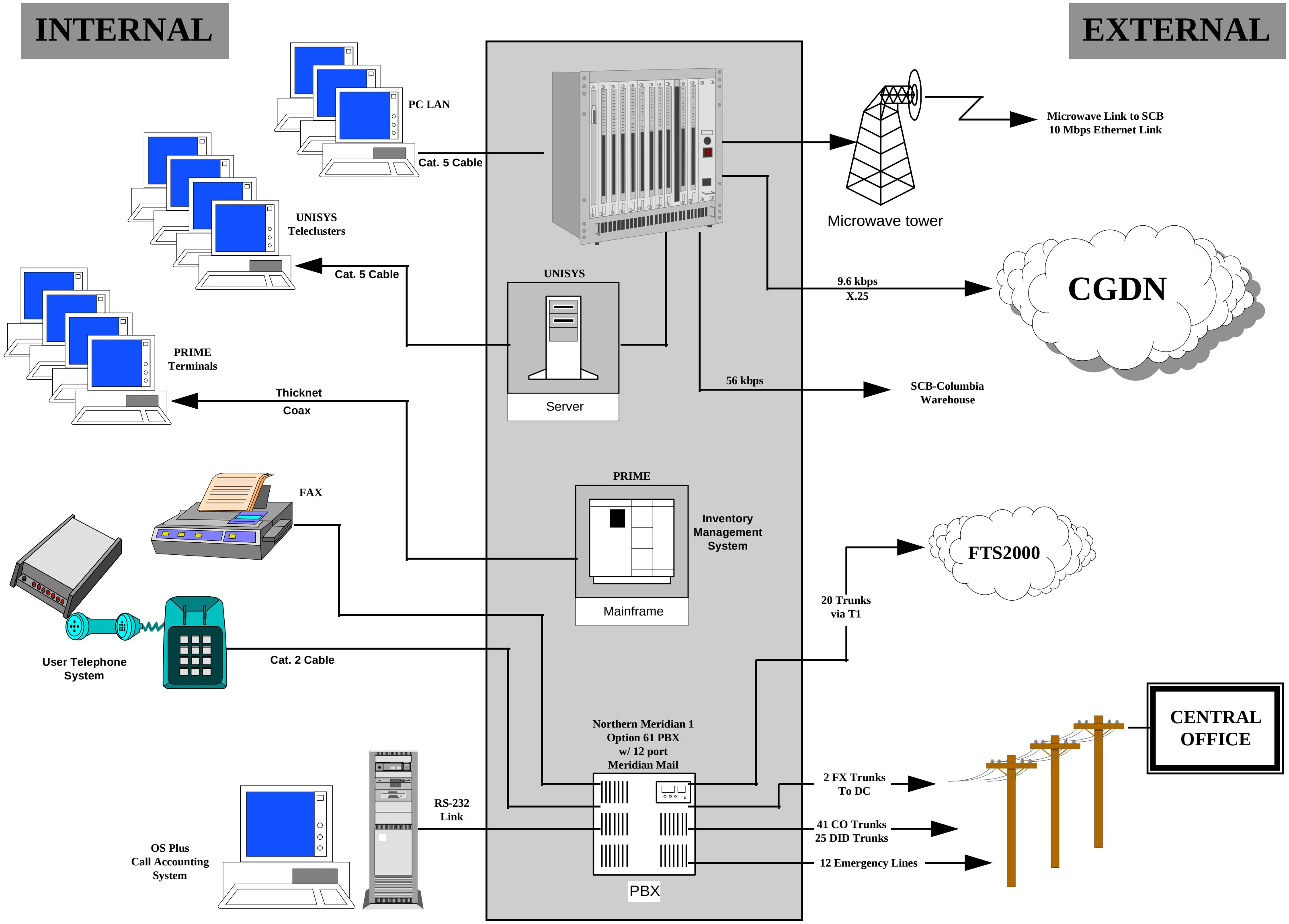
SCCB is located in the Coast Guard Yard, Curtis Bay, Maryland. Their primary mission is the overall management, control, and issue of spare parts to all Coast Guard units. SCCB procures, stores, repairs, and ships specific categories of material, and provides selected technical and logistical information. This includes hull, mechanical, electrical, and ordnance equipment, to the Coast Guard fleet.

The hub of SCCB's voice telecommunications system is their Private Branch Exchange (PBX), where a number of telephone trunks provide service for 304 staff.

The primary component of the SCCB data communications system is the CGSW-II LAN. Category 5 cabling is used from the LAN servers to the closets and from the closets to the desktop terminals. A PC-LAN also is present. The LAN's provide access to CGDN and a microwave link to the warehouse facility at Columbia, MD.

Several terminals connect directly to SCCB's PRIME mainframe computer which houses the inventory management system. Users are connected to the PRIME computer via a Thicknet coaxial backbone. Most of the unit's work is in the logistics databases housed on the mainframes.

Supply Center Curtis Bay



2.6 Contingency Communications

2.6.1 Transportable Communication Central (TCCs)

The TCCs are portable, self-contained communications platforms designed to provide support when temporary communications facilities are required at short notice. There are three TCCs. Two (one at each CAMS) are Transportable Multi-Agency Communication Centers (TMACC) which support joint and multi-agency operations. The Transportable Multi-Mission Communication Center (TMMiC) is located at CAMSLANT and was developed to support Coast Guard missions, but can work with other DoD agencies.

Both types are ground/air transportable. They are self-sufficient except for primary power which is supplied by portable generators or from power lines. Both can be deployed within six hours of tasking. They require one Telecommunications Supervisor for operator training and one electronics technician for support.

The TMACCs (1992) are older and equipped with a broad range of state of the art communications and command and control systems which enables interoperability with Coast Guard, DoD, U.S. Customs Service, Drug Enforcement Agency, and local and state police systems. The Coast Guard has configured them to provide communications over a broad range of frequencies, including satellite, as well as landline connectivity.

The single TMMiC (1996) has a Private Automatic Branch Exchange (PABX) with connections for up to eight phone lines, three of which are patched to a portable cellular system. The TMMiC can act as a mini-command post in the war on drugs or in case of emergencies or natural disasters.

Capabilities shared by both types of TCC's:

- VHF-FM 30.0-50.0 MHz and 138.0-174.0 MHz , DES protected
- VHF-AM 115.0-152.0 MHz, protected
- UHF-FM 415.0-500.0 MHz, protected
- UHF-FM/AM 225.0-400.0 MHz
- HF 1.6 to 30 MHz Voice Mode, SSB, secure and unsecure
- HF 1.6 to 30 MHz Data HFDL Radio Teletype
- SATCOM Line of Sight, Half Duplex
- OTAD capable
- PABX phone system. Two or four wire capable. T1 trunk capable.
- Secure Fax machine
- Standard INMARSAT "A" Voice only

- Cellular STU-III
- Weather Facsimile, NAVTEX capable
- GPS receiver
- CGSW computers with Printer
- Laptop PC, E-mail capable

Capabilities of the TMACC only:

- Customs Over the Horizon Enforcement Net (COTHEN)
- JOTS (TAC3) Receive Only. STU-III Transmit and Receive

Capabilities of the TMMiC only:

- Portable Cellular Site with three cellular phones
- Standard INMARSAT "C" (data only)
- External RS-232 jacks for additional laptop setup

2.6.2 Other CAMS Contingency Equipment

Both CAMS have additional deployable communication systems to support Coast Guard emergency and special operations. These systems include an inventory of :

- Portable DAMA units (SATCOM)
- Portable LCCS-300 suitcase (SATCOM Line of Site)
- Portable INMARSAT "A" Phones (voice only)

2.6.3 District Contingency Equipment

Each district has a variety of portable communications equipment for contingency operations. Usually it is held at the District/Area COMMCEN and issued out as necessary. The following are examples of equipment available from the staffs:

- ERNIE Modems (2 ea. CODEX 5000, X.500) for dial-up connection to CGDN on CGSW-II
- Portable VHF Base Stations
- Portable HF Stations
- Portable INMARSAT Units
- Portable DAMA Units
- Portable LST5s

- Handheld VHF transceivers
- Deployable cellular telephones

2.7 System/Application Matrix

Application	Responsible Office/Division
LUFS (UFS)	G-A
CDB	G-CCS
IBUDS	G-CCS
LAWS	G-L
LEGAL	G-L
MMLD	G-M
MMS	G-M
MSN (MSIS)	G-M
PAWMIS	G-M
ANCRS/CARS	G-O
LEIS II (SEER)	G-O
SORTS	G-O-2
GDOC	G-OCS
SCCS	G-OCU/OCC/SCE
AUXMIS	G-OCX
ELT	G-OPL
ATONIS	G-OPN
LOIS	G-OPN
VIDS	G-OPN
AMVER II	G-OPR
CASP	G-OPR
SARMIS	G-OPR
SARSIM	G-OPR
ATIMS	G-SAE
ALMIS (ACMS, AMMIS)	G-SAE/G-OCA
MPRS (AMP, MSG BD)	G-SCT
MTDS	G-SCT
NAVTEX	G-SCT
SWSAMPS	G-SCT
HFDL	G-SCT/G-OCU
CEDS	G-SCV
IMIS	G-SE
EMAIL	G-SI
DIR/PUBS	G-SII
RADMIS	G-SIR
AIM (PPA, SWIM, EEIS)	G-SLS
FEDLOG	G-SLS
SCCR	G-SLS
STAR (ARMS)	G-SLS
FLS (CM PLUS, SCAMP)	G-SLS/G-AFL
SCAMP	G-SLS/G-AFL
CLAMS	G-WK
KRIS	G-WK
SDA	G-WNI
HDMS	G-WP
PDS	G-WP
PMIS/JUMPS	G-WP

- **Aviation Logistics Management Information System (ALMIS)**

  ALMIS is a Coast Guard system that merges portions of the Aviation Computerized Maintenance System (ACMS) and the Aviation Maintenance Management Information System (AMMIS). ALMIS provides these software links to allow coordination of their maintenance and supply systems. It also provides a projection of the parts that the Coast Guard needs to satisfy their scheduled maintenance. The ALMIS project is connecting the capabilities of both ACMS and AMMIS.

  The ACMS provides the Coast Guard with a system that captures, stores, processes, and reports aircraft maintenance information. Each of the Coast Guard's operating activities provide information about its assigned aircraft, maintenance performed, component failures, mission readiness, and any other key operational data. The system processes the data and generates various operational, planning, and management reports.

  The AMMIS contains information on material requirements that support inventory management activities for the aviation community. AMMIS coordinates with ACMS to provide configuration management and supply information to their aviation forces. AMMIS supports all of the separate maintenance tasks that the Coast Guard needs to track and schedule in support of aviation missions.

- **Automated Mutual-assistance Vessel Rescue System (AMVER)**

  AMVER is a computerized search and rescue network that serves as a safeguard for ships, world-wide. It supports more than 124 nations and every ocean in the world. Every day more than 2500 vessels world-wide participate in the AMVER Safety Network. The AMVER system is a computer generated database that plots significant ship voyage information such as time of departure, destination, turn points, radio call sign, medical personnel, and other relevant information. It can readily locate AMVER vessels and determine their direction of travel. A network of 130 world-wide coastal radio stations relay AMVER position reports to the database at OSC Martinsburg.

- **Aids To Navigation Information System (ATONIS)**

  ATONIS is a system that Coast Guard units use to track and schedule the servicing of their aids to navigation. Districts use ATONIS to perform Local Notice to Mariners (LNM) reports, and AtoN and related equipment inventories. It is used for Coast Guard-wide and district specific queries.

- **Auxiliary Management Information System (AUXMIS)**

  AUXMIS is a Coast Guard program management tool. It is a personnel system to provide Headquarters and Coast Guard Auxiliary leadership with the capability to track, analyze and report Auxiliary activity efficiently. They use the resulting information to coordinate specific activities and to monitor the Auxiliary program. The system maintains personnel information for all of the Auxiliary members. Individual units provide Auxiliary input into a central database. Users of this database can validate this information and produce management reports that support program objectives.

- **Computer Aided Search Program (CASP)**

CASP receives case information and calculates the target location probability cells and reports this information back to the command center. CASP can graphically display this cell information to aid in developing the necessary search paths necessary to support various missions. For SAR missions, CASP can take a range of inputs and simulate a range of possible target locations and then calculate probabilities of success for each search. CASP also provides latitude and longitude coordinates to participating units via AUTODIN. CASP resides at OSC Martinsburg, and Area and District Operation Centers access the system.

- **Fleet Logistics System (FLS)**

FLS is a system that integrates each of the Coast Guard's logistics activities. FLS provides Coast Guard management with increased visibility into these logistics activities and provides senior management with an increased capability to proactively manage their logistics functions. Several subsystems fall under the umbrella of FLS. Two are CM PLUS and SCAMP.

CM PLUS is a unit-level system that links a unit's physical configuration information to related supply, maintenance, and technical information. It allows a unit to manage its configuration data, schedule and record the completion of preventive and corrective maintenance, maintain allowance and inventory information, and requisition material and maintain technical data. CM PLUS interfaces with several on-shore systems and organizations to order supplies, coordinate shore-based maintenance tasks, and report on and analyze cutter performance. It is an integrated configuration-based supply and maintenance system developed to help cutters achieve their supply and maintenance missions by ensuring that an adequate quality and quantity of supplies are available to meet operational needs. The Coast Guard targeted CM PLUS for its six major cutter classes, all new vessel acquisitions, and all standard boats.

The Shipboard Computer Aided Maintenance Program (SCAMP) helps the Coast Guard meet its goal of establishing a centralized supply management system. SCAMP provides an automatic planning and tracking tool for preventative maintenance aboard cutters. It provides automated methods to order parts and update inventory.

- **Geographic Display Operations Computer (GDOC)**

GDOC is a graphical information system that support several Coast Guard missions. It specifically supports SAR missions by enhancing SAR planning through an interface to CASP. GDOC plots SAR patterns and overlays this on an electronic chart, provides the user with the ability to send OPNOTEs, and allows the events to be logged. The Coast Guard is preparing to use GDOC as an aid in navigation aboard cutters and patrol boats. They are also integrating GDOC with other systems as an imaging transmission and display system. The Coast Guard uses GDOC at Area and District OPCENs and they plan to apply the system to all cutters, patrol boats, and eventually groups.

- **Joint Maritime Information Element (JMIE)**

  JMIE is a consortium of several agencies from the Law Enforcement and Intelligence Communities who are working to develop an automated information handling system that allows sharing maritime data. The JMIE Support System (JSS) centrally pools maritime data and makes it accessible to JMIE subscribers. This allows users to meet their individual operational needs, such as narcotics interdiction, smuggling, sea and defense zone surveillance, petroleum traffic monitoring, fisheries operations support, SAR operations, and emergency sealift management. JSS data resides at OSC Martinsburg.

- **Law Enforcement Information System II (LEIS-II)**

  LEIS-II is a database containing information on intelligence targets. It provides automated access to operational law enforcement databases for Coast Guard units. It provides a consolidated decision-support system for their operational missions that supports all of the information needs of law enforcement users. These units access LEIS-II via INMARSAT or dial-up modem via CGDN. Data for this system resides on computers at the OSC in Martinsburg, WV.

- **Large Unit Financial System (LUFS)**

  LUFS is the Coast Guard's procurement and funds management software. They use LUFS at the Unit, Group, District, and Headquarters offices as a tool to develop procurement actions and to report, commit, and obligate funds. LUFS transmits financial and procurement data to the Coast Guard Finance Center (FINCEN). FINCEN updates the Departmental Accounting and Financial Information Systems (DAFIS) with this data and automates the reconciliation of DAFIS balances with local accounts maintained by LUFS.

- **Marine Safety Network (MSN)**

  The MSN is the name given to all "M" systems that are targeted for initial development, architecture redesign, or integration with preexisting systems.

  MSIS is a Coast Guard transactional database for exchange of vessel data concerning boardings, inspections, and violations. Marine Safety field units currently use MSIS for planning enforcement actions, recording resource usage, processing violations, issuing Certificates of Inspection, processing casualty investigations, and issuing documentation certificates. District and Headquarters planners use MSIS data to evaluate mission area workloads and to direct or redirect resources as appropriate. It is a nationwide, interactive database for carrying out marine safety functions. The Coast Guard provides access to this information to over 100 of its field units. The data for this system resides at OSC Martinsburg.

The Vessel Identification and Documentation System (VIDS) is a nation-wide vessel identification system that computerizes the processing of maritime commercial mortgages. Data base contains state and vessel titling and other law enforcement data.

- **Personnel Information Management System/Joint Unformed Military Pay System (PMIS/JUMPS)**

PMIS/JUMPS is the Coast Guard's military personnel and payroll system. It provides military pay information for active, reserve, retirees, and annuitants. The PMIS/ JUMPS server also serves as the data server for all personnel and individual training records for the Coast Guard.

- **Search and Rescue Management Information System (SARMIS)**

SARMIS provides the Coast Guard with its primary means for collecting and storing information relative to all Search and Rescue operations. This system is essential in order to have a true picture of the demands made on the Coast Guard Search and Rescue (SAR) operations and to project these demands in terms of future requirements. The Coast Guard uses this information at various command levels to measure unit workload and effectiveness, determine resource utilization and needs, justify budget requests, analyze system operations for potential savings, and promulgate policies and procedures to more effectively manage the overall SAR system.

- **Standard Automation Requisitioning (STAR)**

STAR provides the Coast Guard with a desktop requisition management system. It allows units to access the system through communication interfaces that range from modem dial-up to satellite-based communications. STAR has import capabilities that allow automatic loading and tracking of all MILSTRIP transactions that various sources deliver to the unit. STAR is the follow on system to ARMS.

The Automated Requisition Management System (ARMS) is a conduit for Coast Guard field units to send MILSTRIP requisition transactions into the Defense Automated Addressing System (DAAS). This system receives status transactions and generates accounting data for transmittal to the DAFIS. OSC Martinsburg is the host site that houses the central server that has been recently modernized and streamlined to support requisition management. This central server receives batch transactions from ARMS users Coast Guard-wide.

- **Supply Center Computer Replacement (SCCR) Project**

  The primary objective of the SCCR project is to address the critical near-term needs to replace obsolete computer systems at Supply Center Curtis Bay. The Coast Guard will consolidate these systems by reusing the Aviation Maintenance Management Information Systems (AMMIS) to the fullest extent possible.

3. FUTURE REQUIREMENTS

3.1 Introduction

In this chapter, we describe the future requirements of the Coast Guard Telecommunications System (CGTS). Our discussion covers the wide range of programs and mission areas in the Coast Guard.

In the following sections, we will describe the key communications requirements, organized by the distinct interviews we conducted, and again by Coast Guard mission area. The results are encapsulated in Table 3-2. It should be noted that these key communications requirements were provided by the programs and organized by mission area. However, the overall final Coast Guard Telecommunications Plan (TCP) must prioritize these requirements to meet the overall grand strategy of the Coast Guard and changing mission priorities in the future. In the last section of this chapter, we will identify the gaps that must be bridged to meet the Coast Guard's telecommunications requirements over the next five years.

For this chapter, we have partially based requirements on input provided by Coast Guard Headquarters Program Managers and Staff. This complements the research and analysis that we accomplished on the site visits during Milestone II (Baseline) and the ongoing review of government furnished information (GFI).

During the interview process, it was clear that many managers have the vision of future Coast Guard operations. Their vision has allowed us to establish some high level communications requirements. Most of the participants, however, have not been able to quantify those requirements in terms of bandwidth. There are a few exceptions that we will highlight in this chapter. Since this is the best mission specific data available to the Coast Guard, we will use it as a baseline to estimate future bandwidth needs on a broad front for the organization.

3.2 Interview Process

Several Program and Support Manager Staffs were solicited for input to the requirements process. As a result, we conducted fifteen separate interviews with various representatives of those staffs. ANTEON prepared questions and the queries were screened by G-SCT. The questions ranged from general solicitations on future views of the Coast Guard's general needs for communications services to specific inquiries about system bandwidth requirements. The replies ran the gamut: validated requirements, not validated requirements, and solutions. In each succeeding section, we have further refined the interviewee responses into requirements that can be validated in the concurrent clearance process. The reports, on each of the interviews, are on file in G-SCT.

The interview questions were developed partially from information obtained during the site visits, and also from GFI, particularly the Command, Control, Communications, Computers, and Intelligence (C4I) Baseline Architecture document. This was done to improve the focus of the interviews and achieve synergy between these two important efforts. The interviews sometimes revealed the existence of more applicable GFI. Where requirements for this additional information was needed, they are referenced in this chapter. Most future requirements for the communications system are not adequately documented. Consequently, in a number of situations, this document will be the first official recognition of these requirements.

3.3 Program Managers' Requirements

This section is the first step towards a consolidation and organization of the telecommunications requirements that are based on the Program Manager interviews and the site visits. The requirements are listed under the appropriate interview heading along with a brief description of each. In some cases the "requirements" appear to be more along the lines of solutions. Occasionally, the interviewees responded in this manner and their comments are represented here. In subsequent sections, we will further fine-tune requirement definitions.

3.3.1 G-A (Acquisition)

Bandwidth Increase: Computer Aided Design (CAD) drawings are large and will take up massive amounts of electronic storage space and bandwidth when electronically transferred from place to place. Data compression will be needed to reduce the size of these documents.

The Facilities Management Information System (FMIS) stores data that aids the Coast Guard with Congressional Question and Answer (Q&A) responses, budget formulation, program descriptions formulation, resource allocation, platform and equipment acquisition, mission performance measurement, and cross functional coordination. This system will increase communications requirements.

There is a growing gap between the current system and future requirements. The current X.25 Coast Guard Data Network (CGDN) has limited speed capabilities. To provide added capacity for lower level Coast Guard units, CGDN tail circuit connections need to be upgraded from 9.6 kbps to a higher speed. The goal from the Information Resource Management (IRM) Board is to have 800 units connected on tail circuits.

An upgraded network with sufficient flexibility and scaleability is needed to provide bandwidth and speed of service to meet all current and future requirements.

Secure Data Communications: Data security is a must. A firewall will be needed between the Coast Guard INTRANET and the INTERNET to maintain security.

Electronically Maintain Documents: Shipyard information and documents (i.e., engineering and technical drawings; configuration management reports, etc.), currently stored on paper copy and blue prints, need to be placed on-line via electronic means and stored in a database.

Electronic Access to Reference Materials: Access to the INTERNET is required for interface with contractors. Some type of querying technique would be preferred. Moving the Major

Acquisition process to the WEB will save time and mailing costs. To interact with the Coast Guard acquisition program, contractors will need INTERNET access. Major acquisition activities, including Request For Proposals (RFPs), Q&As, and proposals, will all be handled, in the future, via the INTERNET. G-A wants to be able to perform key word searches on these documents. Beginning in the near future, contractors will only be able to do business with the Coast Guard electronically. These requirements will be implemented over the next year or so.

Technical publications are managed on CD ROM now. There is movement toward placing technical publications on the INTERNET, allowing them to be managed, distributed, and accessible on the INTERNET.

Video and Imagery: Video and imagery services will be needed at major units to meet acquisition process requirements. Many of the processes, currently being operated at Project Resident Offices (PROs), will be moved to the Fleet Logistics System (FLS) in the future. PROs will be transferring CAD files back and forth.

Upgrade CD ROM Capabilities: G-A has CD ROM capabilities. These capabilities provide an inexpensive access method to large amounts of reference material.

Video Teleconferencing: G-A would like to see video teleconferencing between Headquarters and the PROs. Video teleconferencing costs will be off-set by savings from reduced travel requirements. No solid requirements for video teleconferencing currently exist in the Coast Guard, and no regulations or standards are in effect concerning video implementation. G-A believes that no formal study has been completed to date. (Note: A video teleconferencing pilot project and study was completed by TISCOM and G-SAE in October 1995 which supports the conclusions expressed by G-A.) However, under the current budget climate, G-A believes video teleconferencing can benefit the Program by saving travel time and reducing travel costs. They also believe that if standardized video technology was available, video teleconferencing would be more widely used.

On-Line Access: One requirement that must be included in FLS is on-line access to the Federal Acquisition Regulations (FAR). INTERNET access may be one way to meet this requirement.

3.3.2 G-CFP (Finance and Procurement)

Bandwidth Increase: The Large Unit Financial System (LUFS) is one of the most active CGDN users. The CGDN is a store and forward type network, and seems to handle the traffic load well. However, LUFS is moving to a near real-time requirement. Increased bandwidth is needed to meet this criteria.

Speed of Service: Many users consider the store-and-forward CGDN to be unreliable because of problems with delayed and/or lost messages. Improved system reliability and speed of service is needed.

A less "primitive" process of network operation is needed to lessen the burden of using alternative methods, such as mail and facsimile, which are being used extensively throughout the Coast Guard.

"Real-Time" Service: Certified sites on LUFS have a "near real-time" requirement. Units need to have access to real-time budget and expenditure data.

Flexibility and Scaleability: To best meet user requirements, G-CFP needs a network solution that is both flexible and scaleable.

Information Exchange Policy: Policy is needed to help control file transfer and circuit use for software programs such as Microsoft Exchange Mail. Information packages being transmitted over the network are rapidly growing in size and frequency. Hardware on the current network is not designed to handle the anticipated load requirements.

Some control over the number and content of Coast Guard WEB pages is needed.

More control and monitoring is needed for e-mail and attachment file size to prevent problems. Large documents with imbedded spreadsheets, etc. will tend to bog down the network. Policy is not the solution by itself. Monitoring (policing the network) needs to be done to prevent abuse of the system.

Centralized Database: Move to central databases to avoid the local complexity of the client-server environment.

INTERNET: Aircraft maintenance drawings, currently being maintained by the Department of Defense (DoD), are being moved to the INTERNET. This means that Coast Guard units will need to use INTERNET to access the drawings. Units will also need INTERNET access for training purposes.

Automated Procurement System: G-CFP is moving away from the current paper intensive procurement system toward an automated on-line system. Small purchases should be performed at decentralized locations. Executive order mandates that all procurement transactions will be accomplished through electronic commerce (EC) in a paperless environment.

For automatic financial transactions, payment authorization should be at the same level as procurement authority. Payment status should be available through on-line queries and final payment documentation should be automatically provided to the contracting officer.

Consolidated Management Reporting System: Commandant needs a database that tells him how well the Coast Guard is functioning. In naval engineers parlance this is a "gauge board." This has been the objective of the Corporate Database, where operational and budget information are consolidated to provide a strategic Decision Support System (DSS) for the Coast Guard.

INTRANET: This is a network, or group of networks, within an organization, connecting the organization's members and employees to a range of computer services, resources, and information. A set of network conventions and common tools are employed to give the appearance of a single large network, even though the computers that are linked together may use many different hardware and software platforms. “Firewall” protection is provided to limit the exposure of the network to an attack from an external location. Routers and other internetworking devices use their access control capabilities to build firewalls that can prevent unauthorized entry from outside sources.

Table 3-1 shows some of the major differences and commonalities between INTERNET and INTRANETsystems.

Table 3-1: INTERNET vs. INTRANET

Parameter	The INTERNET	The INTRANET
Security	Low (None/Some)	High
Speed	Low/Medium	High
Services	Almost unlimited	Specified by Organization
Access Control	None or limited. Public encouraged to visit.	Account Name and Password. Generally no external (public) access.
Membership	Unlimited. 50 +/- 20 millio	Population of Organization
Reliability	Low	High (Mission Critical)
Control	Low (None)	High

***Automated Asset Management System**:* An automated asset management system is needed which integrates all Coast Guard property into the centralized tracking system. Property should be accounted for electronically and accessible to all units through on-line query capabilities.

A fully integrated finance and procurement information system is needed which supports decision-making, and satisfies data calls and reports for both internal and external sources.

***One-Time Data Entry**:* One-time data entry 100% of the time is the goal. Access to current financial and procurement data should be available 95% of the time. Corporate systems need to be developed to reduce manual data calls by 90%.

***Imagery**:* Requirements exist for graphic images and digital pictures. This includes plans and drawings for contractual negotiations.

***User Pull**:* The ability for authorized personnel to access and/or download data, such as message traffic, directives, publications, contract information, and training materials for operational or administrative purposes, is needed. Users want to do their own driving on the information super-highway. They would like to have more control over the movement of data, and would prefer to have the capability to “pull” information, when they need it or when it is convenient for them to receive it, instead of having information “pushed” at them. User Pull from a WEB page is needed.

***Digital Signature Standard**:* There is a need to go to a digital signature standard.

3.3.3 G-L (Legal)

INTERNET: The most immediate requirement is to move away from the costly use of the legal database, LEXUS, and/or CD ROM, and go to the INTERNET. Explore those cases where we can obtain INTERNET access to legal data vice having to pay for LEXUS.

***Centralized Database*:** Currently, a stand-alone terminal is used at remote sites for tracking time and usage data. Under CGSW III, a stand-alone terminal will still be used.

G-L would like to see a shift to INTRANET or a Distributed Database (DDB). A centralized or replicated database on the system is a requirement.

INTRANET: Move away from CD ROM to a more immediate on-line capability.

Electronic Transfer of Documents: G-L wants the capability to electronically transfer documents.

Secure Data Communications: Protection for sensitive information is a requirement.

Imagery: G-L does not see a drastic increase in the use of imagery, within their Program, over the next five years. (Litigation may require some imagery for criminal proceedings.) However, the need for imagery may increase as the capability increases.

3.3.4 G-M (Marine Safety and Environmental Protection)

Bandwidth Increase: In the future, more bandwidth will be needed to compensate for an increased amount of data queries from program management personnel, and a real-time imagery requirement from the Marine Environmental Protection Program. Some applications, such as Marine Safety Management System (MSMS), which currently reside at Headquarters, may move to Operations Systems Center (OSC) Martinsburg. As a result, there needs to be a "huge" pipe from Coast Guard Headquarters to OSC Martinsburg to handle the load.

Bandwidth on Demand: In the future, the demand for data will increase in all areas. Sufficient bandwidth is required for graphics based transfers of large files, such as electronic ship building plans, etc.

Increased Speed of Service: Marine Safety Information System (MSIS) uses the CGSW II as a "dumb" terminal. This causes a high communications rate with heavy amounts of data going back and forth between the user and the host computer. The length of time it takes to get information back and forth is the biggest problem for "M" users. It is not the communications pipe itself that is causing delays. It's the Central Processing Unit (CPU) or host unit processing time. CPU and/or host unit processing time needs to be improved.

Interoperability: A primary requirement for G-M telecommunications is the ability to interface with other government agencies, state and local authorities, and private sector entities, such as those involved in spill clean-ups.

Remote Access: The new CGSW III will expand the use of remote computer access, and information will be available electronically via dial-up or other means. Some information, such as publications and directives, will not be available on MSIS. This capability may be provided for on the Coast Guard INTRANET.

Dial-in Capabilities: There will be an increased need to dial-in to OSC Martinsburg. Detached duty inspectors, telecommuters, and work-at-home after-hours personnel are examples of users that will require this capability.

INTRANET: On-line field guidance is desired in an INTERNET-like environment. There is a need to interface with the public and third party professional institutions, such as American Bureau of Shipping.

Imagery: Imagery capabilities are needed. On-site case information (Marine Environmental Protection (MEP), casualty investigation, etc.) may be required in real-time imagery. The "pipe" must be large enough to handle it.

Short Range Radio Communications: There is still a need for Very High Frequency-Frequency Modulation (VHF-FM) communications with Coast Guard small boats during oil spills, etc. VHF command and control system improvements, such as filling in the coverage gaps and cellular phone communications in emergency environments, are needed.

3.3.5 G-OC (Operational Facilities)

Bandwidth Increase: Improvements need to be made in the current system. The current system does not effectively move large volumes of data in a timely manner, at least not without generating excessive manpower requirements. It is very labor intensive to send traffic on the current system, and even routine information becomes critical because of excessive delays. For example, the length and complexity of the typical MILSTRIP message makes it very labor intensive and causes delays in message delivery.

Greater bandwidth will be needed to take all-source intelligence information farther down into the organization. This means greater bandwidth requirements while moving towards a common system. Different classifications should use the same pipe.

The Coast Guard needs to transition to new technology with DoD, and they need to ensure there is enough bandwidth available in any DoD migration plan.

It is important that a "surge" capability is built into the bandwidth requirements and included in the system design.

Common Tactical Picture: In a multi-unit environment (ships, planes, and boats), on-scene units, typically the On-Scene Commander (OSC), require the ability to seamlessly and rapidly pass along mission status information and situation reports to oversight personnel ashore (e.g., the Search and Rescue (SAR) Mission Coordinator (SMC); Operational Commander). This could best be accomplished electronically by transmitting a common tactical picture to all concerned, which clearly and accurately depicts the current situation. The least man-power intensive display methods are required.

Funding for cellular and satellite phones is a "requirement." A common telephone may be the answer (i.e., a data link with laptop computer via cellular phone). A tactical picture during major operations is very important.

Global Dial-Tone: Users will have the capability to communicate with anyone anytime using a single workstation (for all data needs) or telephone (for all voice communications).

Automated Systems: "Automatic information" is needed. This means that data submissions, where information is summarized and reported for SAR cases, law enforcement operations, floods, disasters, fuel/provisioning logistics information, etc., should be prepared only once, transmitted, received, logged, and displayed automatically without human intervention.

The automatic feature is important. We need to get the operator out of the loop. Message traffic is a "paradigm." The Coast Guard needs to rely more on automatic delivery of information. For example, automatic transmission of positioning information for aircraft is needed. The trick is finding a pipe that can handle everything.

Interoperability with Other Government Agencies (OGAs): Interoperability with OGAs is required for large SAR cases and many other major operations. Multiple display of information across agencies is needed. No current system exists that will marry the Coast Guard with local law enforcement agencies. There is a need to work with other agencies using a common situational picture. Satellite data links and cellular phones need to be linked together and they need to be able to operate in any environment.

Video and Imagery: There is a need to have one common pipe for all pictures, and the pictures need to be "faster." They need the ability to overlay one picture to another without having to transmit numerous pictures several times. On-site case information (Enforcement of Laws and Treaties (ELT), SAR, etc.) may be required in video clip or imagery format. Imagery is needed for national intelligence information. G-OIC is interested in obtaining a copy of all non-public affairs imagery, that is collected, for their library in a centralized server located at the Intelligence Coordination Center (ICC).

A standard "resolution" for imagery should be established.

An increasing requirement is the availability of a clear situational picture of operations during National Crisis.

Inexpensive, Reliable, and Efficient Communications: Develop a better solution than the expensive International Maritime Satellite (INMARSAT). INMARSAT is not the way to move logistics information. It's too expensive. There is a lack of competition in the commercial satellite communications (SATCOM) arena now, but that is going to change. As a result, the cost should come down in the future. Technology-wise, some operators will say that INMARSAT is not that good and connections tend to be unreliable. However, it has plenty of bandwidth and is more reliable than traditional High Frequency (HF) communications. HF has many technical problems and most operators will agree that INMARSAT provides much better voice quality and overall service than the typical HF phone patch. High Frequency Data Link (HFDL), originally designed for delivery of operational message traffic only, is much too slow to meet growing traffic load requirements, and frequent backups of message traffic are common place. Currently, there is no better solution (albeit expensive) than INMARSAT. (The Coast Guard has access to Military Satellite Communications (MILSATCOM) based on operational requirements and interoperability needs with the U.S. Navy. MILSATCOM may, in certain cases, be a viable alternative to INMARSAT.)

Telecommunications support for the Intelligence Program needs to be increased, specifically for Law Enforcement Detachments (LEDETs) and other field intelligence units.

Most systems are shifting to Transmission Control Protocol/Internet Protocol (TCP/IP). This surfaces a problem of how to get data to the ships with TCP/IP. A larger pipe is needed.

Efficiency Improvement: Reduce the amount of replication of information which appears to be everywhere. The system is overcrowded. The speed of service is too slow. System efficiency (sharing of information) does not meet user needs. The system can't handle the high volume of traffic (greater bandwidth requirements are imminent from anticipated new applications).

One-time Entry of Information: Users do not want to re-key information. They want to enter it one time into the system.

Operations Information System: The capability is needed to automate and standardize operational reports.

To improve efficiency, automatic information is needed to ease the job of boat coxswains and other operational personnel. There is a need to get a tactical picture to small boats underway for SAR cases, etc.

Data Security: There is a need to "get past the air-gaps." Security requirements need to be addressed, for example, where classified information, such as Officer-in-Tactical Command Information Exchange Sub-system (OTCIXS) data, needs to be displayed on the bridge. Multi-level security is needed to merge unclassified and classified traffic onto one terminal (e.g., marry the Secret-high Local Area Network (LAN) in both Areas with Secret Internet Protocol Router Network (SIPRNET)).

Automated Chart Updates: Cutters need automated chart update capabilities while underway for safety of navigation purposes. There are numerous standards pertaining to programs for transmitting information of this type. The telecommunication system will be tapped to accommodate this. It needs to be reliable. There is a future requirement to update charts by data burst via the telecommunication system. They are updated manually now. The Navigation Center (NAVCEN), Alexandria, Virginia may be assigned the responsibility of transmitting the updates.

***Satellite Communications**:* Satellite communication capability is needed between cutters and aircraft. To provide interoperability, a gateway at a "fusion" site may be needed vice putting equipment/systems on every unit in the Coast Guard. As a result, less equipment will be needed on each unit. Units will have only what is needed to talk with the "fusion" site. CAMSLANT or CAMSPAC may be the best fusion sites for record messages and phone patches. They may also be good sites for increased capabilities in other areas.

***Solution to Cutter Antenna Interference Problems**:* There is a requirement to fix antenna interference problems on cutters. The problem is too many antennas, too little space.

***User Pull**:* We need to examine how information can be sent to or "pulled" by the user more effectively and efficiently. Pulling and sampling information is very useful. "User Pull" of information is needed.

Users need the capability of "pulling" intelligence information with other information.

***Direction Finding Capabilities**:* Direction Finding (DF) capabilities are needed in the National Distress System (NDS). This capability is required to locate vessels in distress and possible law breakers within the range of NDS.

3.3.6 G-OP (Operations Policy)

***Bandwidth On Demand**:* The telecommunications system needs to provide "bandwidth on demand" to both shore units and mobile units. Ideally, the user should not feel that communications are constrained by the communication path or the high cost of the communication.

***Bandwidth Increase**:* The most significant gap in the current system is the lack of affordable and reliable communications bandwidth to Coast Guard mobile units.

Bandwidth is needed to meet future increases in the exchange of information with the public.

NAVCEN is looking at future requirements for moving data. They currently have simple, low-bandwidth requirements that may not change much in the near future. However, improved circuit availability is needed between NAVCEN and Telecommunications and Information Systems Command's (TISCOM's) demark. Because outgoing and incoming NAVCEN traffic has to pass through this local circuit, NAVCEN is experiencing a bandwidth bottleneck at TISCOM. They have had no major delays to date, but there is still an availability impact.

***Interoperability**:* In the future, NAVCEN will provide a number of navigation information services to the public. The public will be able to access information via a dial-in system or through the INTERNET. This service will include Differential Global Positioning System (DGPS) status information and notice to mariners. Information will be provided on an INTERNET Home Page and also posted on a bulletin board. Facsimile (FAX) services are now available, and remain as a requirement.

***Mobile Communications**:* Affordable and reliable communications bandwidth, to all Coast Guard mobile units, is needed.

For ice operations, capability is needed to communicate with a centralized database, real-time, from aircraft and vessels.

Data Security: Password security will be required. Secure communications are needed.

***Short Range Radio Communications**:* The Coast Guard will need to be able to receive a distress call from a boater who is using state-of-the-art equipment or any other widely held standard communication system.

VHF used to be the primary means of short range communications. Now short range communications have become more complicated. For example, satellite links are increasingly used as a means of ship-shore communications (i.e., American Mobile Satellite Corporation (AMSC), INMARSAT, and others coming on line) along with cellular phones. The public will go with the least expensive means available to them, and the means selected may not always be two-way communications. It may not even have a SAR alerting capability. The Coast Guard needs a mechanism to be able to continue to receive distress alerts and maintain two-way communications with the public.

Global Maritime Distress and Safety System (GMDSS) was designed for the commercial mariner and is not a requirement for the public boater. Most of the Coast Guard's SAR and law enforcement customers are not regulated by GMDSS. Commercial fisherman are not covered under Safety Of Life At Sea (SOLAS), but make extended voyages out to sea. The NDS encompasses the near-shore coastal environment. The public boater is moving towards using cellular telephones for distress where the boater will dial 911 or *CG if he gets in trouble and needs assistance. This may or may not work well. There is no guarantee that the caller will get through and cellular phones do not have the "all-call" feature that VHF radio has always provided.

***Query Database**:* Coast Guard Headquarters needs the capability to query operations information directly, instead of the current methods of sending mail, etc. One-stop-shopping is the requirement. Information queried does not have to be resident in the on-line transactional databases. The on-line database can be replicated to provide a stable historical database for internal or external customers.

***"Near Real-Time" Information Exchange**:* The Program Manager would like to see near real-time input and real-time output of data. This may eliminate the use of forms.

Response time is important in the use of a central database. Currently, "batch" input is used for Aids To Navigation (AtoN) aid changes and corrections. However, for Navigation Safety information, there is a need for near real-time input, to the central database, of changes and corrections from the mobile platforms. Aircraft and small boats can enter data on their local onboard terminal. When they land or return to port, they can download their stored data to the central database.

There is a requirement to maintain up-to-date technologies for the Navigation Information Service (from NAVCEN) that will require them to gather, process, and disseminate timely information to a wide variety of users.

An improvement is needed with respect to command and control capabilities for DGPS sites and Loran Stations. Extremely robust and reliable communications are needed for remote control and casualty recovery of the equipment used at these sites to maintain critical radionavigation system availability.

Consolidated Databases: A "combined database" is required for operational units to access, allowing information to be obtained on SAR, law enforcement (L/E), and all other operations.

Centralized Database: There is a need for a central database across all Operations programs. Currently, "batch" input is used for Aids to Navigation (AtoN) aid changes and corrections. However, for Navigation Safety information, there is a need for near real-time input to the central database of changes and corrections from the mobile platforms. An improvement is needed to command and control capabilities for DGPS sites and Loran Stations. The future requirement for the Aids To Navigation Information System (ATONIS) is a capability to communicate with a centralized database. A communications capability will be needed to process and disseminate information to a variety of interested parties from that database (i.e., Notice to Mariners, Light Lists, etc.). ATONIS itself may be centralized.

Aircraft and small boats can enter data on their local onboard terminal. When they land or return to port, they can download their stored data to the central database.

Field Query of Database: The SAR Database is being modified and will be moving to OSC Martinsburg. Field units currently submit information electronically via modem/landlines to their present District Office, who in turn submits the information to Headquarters. The field can only access the database at the District level. However, this is not a user friendly method, and consequently the database is seldom accessed. The field needs the capability to query the central database on a routine basis. The database needs to be designed for one-time input and real-time output. Timely database updates with current SAR case data will be required. Units need to be able to view information that pertains to their unit, along with some overall composite information that pertains to all units.

Public Access to INTERNET Database: NAVCEN may, in the future, be the public INTERNET interface to Coast Guard databases. To do so, they expect to have a dedicated T1 line to OSC Martinsburg's databases from which they will frequently update their local databases. (NAVCEN expects to operate several Coast Guard databases.) The public will have limited access to database information, and only be allowed to access information residing at NAVCEN. This will protect the integrity of database information residing at OSC. NAVCEN is not interested in managing databases, just disseminating information to the public.

There is a requirement for a gateway from the Coast Guard's INTRANET to the INTERNET. A decision needs to be made as to whether the gateway will reside at NAVCEN or at OSC Martinsburg.

***One-Time Data Entry**:* The end-state should provide for one-time entering of data with no duplication of entries.

***Automated Chart Updates**:* Cutters need automated chart update capabilities while underway for safety of navigation purposes. There are numerous standards pertaining to programs for transmitting information of this type. The telecommunication system will be tapped to accommodate this. It needs to be reliable. There is a future requirement to update charts by data burst via the telecommunication system. They are updated manually now. NAVCEN may be assigned the responsibility of transmitting the updates.

***Automated Reports**:* Automate manpower intensive functions like sending position and operations-normal reports, and forwarding SAR and L/E information to a central database.

***User Pull**:* User pull of data can be used for AtoN, SAR, and L/E.

***Imagery**:* There are some imaging requirements for vessel sightings in law enforcement operations, but the Program is undecided as to whether they need vessel names and numbers or a picture.

3.3.7 G-SE/SLS (Engineering and Logistics)

***Mobile Communications**:* The requirement is to "move data." There is a need for efficient and reliable data communications with mobile units. Mobile units need the ability to effectively coordinate logistics support while underway. This includes obtaining critical parts and materials in a timely fashion. Currently, mobile units use INMARSAT, cellular telephone, public telephone system, basic radio communications systems, or any other method available to tap into asynchronous communications to access OSC Martinsburg for updates to systems such as FLS. These methods satisfy their current needs, but fall far short of meeting their five year plan.

***Bandwidth Increase**:* The current system pipe size is too small to meet Program Manager requirements. Program Managers are using facsimile instead, to meet speed of service requirements. The existing system will not support near real-time transmissions. CAD files average 1 Mb in size. E-mail attachments are currently used for updates to the Civil Engineering Data System (CEDS). It contains approximately 200,000 records. A series of file extractions are entered into the database once per quarter. This needs to be changed. Records fed up from the field average about 40 data attributes at 400 bites per attribute. Each quarter, 10,000 changes at 400 bites per change equals 4,000,000 bites quarterly. There will be approximately 16,000,000 bites per quarter with the new system. Also, there will be day-to-day data runs on CEDS. The Program wants to do updates daily, as changes occur.

Real-Time Information Exchange: For the most part, the FLS turnaround requirement is approximately one week. Data is stored in the database until a ship calls in with its weekly upload of data. Casualty report (CASREP) requirements are near real-time (within 6 hrs.). The procurement data resulting from these CASREPs requires near real-time response.

Distributed Database: There is a requirement for increased capabilities to effectively exchange logistics support information. Currently, data goes back and forth, but reports are on paper. To save costs, ships underway only send FLS data in unusual situations, not for scheduled items. Also, the whole database is never sent, only the data that has changed.

Centralized Database: Each Civil Engineering Unit (CEU) has a CEDS database of their own. The database gets larger as it goes up the chain of command. A central database is needed. CEDS may merge with the CAD system, in the future.

Consolidated Management Reporting System: The Commandant needs a database that tells him how well the Coast Guard is functioning. In naval engineers parlance this can be represented by a “gauge board.” Figure 3-1 on the next page gives an example of how a Coast Guard corporate database might look to the Commandant. This has been the objective of the Corporate Database, where operational and budget information are consolidated to provide a strategic Decision Support System (DSS) for the Coast Guard.

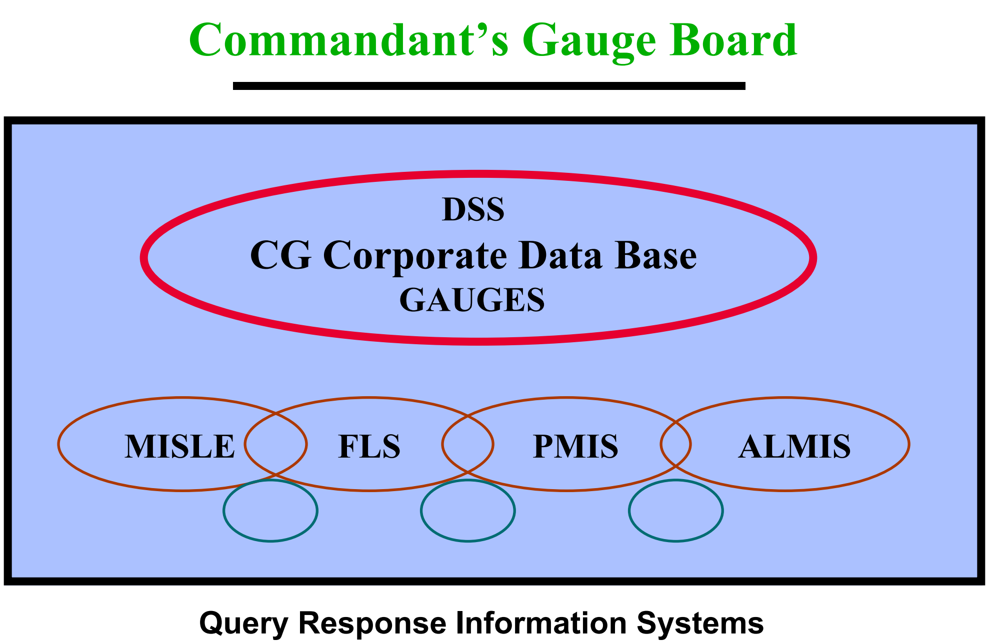


Figure 3-1: Gauge Board

Automated Procurement System: The tendency is to move away from the paper intensive procurement system in use today toward an automated on-line system. Civil Engineering contractor shops may use Electronic Commerce (EC), in the future.

Global Dial-Tone: Users will have the capability to communicate with anyone, anytime using a single workstation (for all data needs) or telephone (for all voice communications).

***INTERNET*:** Currently, new software developed by the Coast Guard and new applications are sent to field units on floppy disks. There needs to be a more efficient method to electronically distribute new products and upgrades. WEB pages are being used to publish status information now, and it appears this method works very well. An INTERNET type system may be the solution.

***Information Exchange Policy**:* With CGSW-III, users have the capability to send extremely large data files over the network (i.e., scan in 30 Mb files to e-mail). To keep system costs down, there needs to be some control over system use, and there needs to be a way to identify abusers of the system. Formulation of policy is the solution. However, policy will only work if abusers can be readily identified and stopped.

User-Pull: The capability for users to obtain information, such as routine message traffic, publications, and instructions when they want it, is needed.

Dial-up Service: Dial-up service to the Civil Engineering Units (CEUs) would provide the capability to send Shore Station Maintenance Requests (SSMRs) electronically.

***Imagery and Video**:* In the future, Civil Engineers will have several imagery requirements. Blue prints, drawings, and plans will be sent electronically.

3.3.8 G-SEA (Aviation Engineering)

***Bandwidth on Demand**:* Applications, such as the Aviation Logistics Management Information System (ALMIS), which merges portions of the Aviation Computerized Maintenance System (ACMS) and the Aviation Maintenance Management Information System (AMMIS), need plenty of bandwidth and modernized LANs in order to provide information connectivity to users across all Air Stations. There will be an even greater bandwidth requirement, as users start to access a central storage site from remote locations to view and obtain information from a number of sources, such as the Directives and Publication System, via the future Coast Guard INTRANET. In addition, more work will be done in a graphics based mode (as opposed to the current character base), and live video capabilities will be needed for multi-media technology.

***Increased Speed of Service**:* Reduce ALMIS response times (for complicated queries) down to 7-10 seconds.

***Operations Information System**:* Aircraft need the capability to automatically broadcast flight information (hours flown, ops normal reports, etc.) to all concerned.

***INTRANET**:* INTRANET will replace CD ROM as the primary document storage and retrieval system. Users will access a central storage site, from remote locations, to view and obtain information from a number of sources, such as the Directives and Publication System. Additional bandwidth will be needed for INTRANET operations. A Browser look and feel would greatly facilitate access to management information contained within ALMIS.

Distributed (Query) Database: Users must be able to run queries without digging into the operational database. The capability is needed to run separate data queries from an on-line transaction based system. ALMIS would migrate from its current host based system to a distributed architecture over a frame relay network employing TCP/IP routing.

INTERNET: There needs to be clear Coast Guard policy on INTERNET use.

Video: Video is needed for multi-media technology (publications, directives, etc.).

Imagery: The ability to move images from aircraft to ship or shore facilities is needed. For example, the HU-25B would transmit oil spill imagery via data link and network connections to MSO representatives.

LAN Improvements for Source of Data Entry: In order to complete Wide-Area Network (WAN) upgrades, the individual Air Station LANs require rework. Many have fragmented architectures and lack a cohesive Category 3 or 5 wiring infrastructure. ALMIS will require modernized LANs in order to provide information connectivity to users across all Air Stations. Fragmented LANs introduce complications in TCP/IP address schemes as well as an inability to move to a less paper intensive environment.

Standardization for DoD Interfaces: The Coast Guard is inextricably linked with DoD in aviation logistics. In order to connect with their systems, many individual initiatives are undertaken, each with its own Automated Information System (AIS) Proposal and level of success. Perhaps a Coast Guard centralized liaison with the Defense Information Systems Agency (DISA) would more effectively shepherd our needs to work with DoD.

Telecommuting: Department of Transportation (DOT), as the National Performance Review (NPR) designated telecommuting sponsor for the Federal Government, has instituted several initiatives. G-SEA would gain many efficiencies through a telecommuting capability now absent from our resources.

Video Teleconferencing: G-SEA sponsored the Video Teleconferencing (VTC) Pilot project and gained real staff resource savings. G-SEA has continual requirements to coordinate with its sister unit, the Aviation Repair and Supply Center (AR&SC) in North Carolina, and continues to depend on this resource.

3.3.9 G-SC (Computers, Communications, Electronics)

Open Systems Architecture: Users of the future communication system need the capability of passing information anywhere, anytime.

Bandwidth on Demand: To meet network flexibility and scaleability requirements, install “big pipes” up front with more capacity than is currently needed. This may yield a savings, in the long run, by not having to incrementally upgrade the circuit to meet increasing user requirements over the next few years.

Inexpensive, Reliable, and Efficient Communications: Solve the short-falls of ship data communications. Commercial satellite communications alternatives, such as AMSC, are being tested now. However, AMSC currently offers no secure communications capability and the status of its future availability is unknown at this time. INMARSAT has proved to be too slow and expensive.

Electronic Mail: Adopt Defense Message System (DMS) products for use in the Coast Guard. A new e-mail policy will be tied to DMS implementation.

Video and Imagery: The drivers in the long term network are the need for video and imagery (tactical data). Video teleconferencing capabilities are not needed now, but on the horizon. It is the best substitute for actual face-to-face meetings. It allows unit commanders to meet with operational commanders with minimum disruption of operations. A 128 kbps pipe system can provide full motion video. Headquarters is currently using 384 kbps. Video would have many applications, such as engineering site surveys and safety investigations. However, video brings with it a demand for more bandwidth. The cost may be less in a few years. The need for secure imagery will drive the data network.

Short Range Radio Communications: G-SC believes the Coast Guard may not totally eliminate the requirement to provide Medium Frequency (MF) and VHF radio communications services with the maritime public. The market is too large.

Implement a robust GMDSS. . . A satellite-based system will not be available anytime soon.

Centralized Database: A centralized look at all systems is needed. Currently, there is no control over the use of the "pipes" (T1 lines, etc.)

Database Replication: As an integral part of the network design process, planners need to take a close look at how database replication capabilities are implemented.

INTERNET: Move towards WEB technology. There should be a significant savings in life cycle costs by having the ability to transfer and use data from a centralized location.

Remote Access: Remote access capabilities are needed (Temporary Additional Duty (TAD), after hours from home, etc.). This may be a dial-up system that can be accessed from various locations not connected directly to the WAN.

Ships need state-of-the-art messaging capabilities. Ships are using HF and SATCOM as their primary record message service. These services, in many cases, do not meet their messaging requirements. Ships need to fit in smoothly to the future network plan.

Ships need more near real-time data. The Coast Guard is fielding a command and control architecture based on the Shipboard Command and Control System (SCCS) for 210s, 270s, and

378s. Track and sensor information is currently being passed via several means (i.e., Link-11, HF, and SATCOM (OTCIXS)). OTCIXS works well for near real-time tactical pictures, and it is a big step forward for the Coast Guard. It would be good to push capacity down below the 210 level, but the technology is not yet available and space is tight on smaller vessels.

Telecommuting: There will be an increasing demand for telecommuting capabilities.

Data Compression: The ability to compress data will increase network efficiency by increasing the throughput without increasing the size of the pipe.

Global Dial-Tone: The command and control system needs a reliable dial-tone capability and a phone book. Global Dial-Tone is the future concept where one telephone set can be used to talk with anyone, anytime. Services, such as the public telephone system, cellular telephone, radio, and satellite systems will be all linked together by intelligent gateways. This concept will also provide similar service for data and video transmissions. As technology becomes available, the Coast Guard should take the command and control architecture to the point where units have that capability... a large undertaking.

3.3.10 G-SI (Information and Technology)

Mobile Communications: More tactical and situational information is needed on mobile units. However, retransmissions of the whole picture, each time an update is required, is not needed. Transmission of the changes, since last update, would be a more efficient method.

A more effective interface is needed for exchanging information between larger Coast Guard platforms, that support the SAR mission, and shore facilities (Districts and Groups) and smaller platforms (WPBs and small boats). Data Encryption Standard (DES) protection, for voice transmissions, is currently being used for special operations.

Identify a better, cheaper, faster alternative to INMARSAT. Other alternatives exist or are planned that may address the Coast Guard satellite requirement. These include the Iridium Project, a network of Low Earth Orbiting Satellites (LEOS), and AMSC.

Improved connectivity to deployed ships is also a requirement.

Icebreaker Communications: Icebreakers need to effectively and reliably communicate or exchange data on a continuous basis, with continental United States (CONUS) based facilities, from the polar regions. This should include the ability to reliably communicate with their operational commander and provide data communications support to scientific teams which are the primary customers of the icebreakers.

A communications transport path is needed to get ice surveillance information (i.e., satellite imagery or reconnaissance information from aircraft; position and drift data; etc.) to operational planners (Districts and Groups) and cutters.

***Scaleable Network**:* The network must be structured so that rapid adjustments can be made to the size of the "pipe" to meet changing user requirements. If a user needs a change, then the bandwidth of the circuit can be increased or decreased appropriately.

***Reliability**:* Provide information to the right people at the right time, so they can make decisions.

Enhancements are needed to the present telecommunication system that will emphasize economy, interoperability, security, automation, ease of maintenance, and improvement of high volume message handling and throughput.

***Bandwidth Increase**:* Increased bandwidth availability and security is needed.

***Data Security**:* Improved network security is needed. The architecture is the key. Firewalls will also be needed.

Virus protection is another important requirement associated with an open system environment. Policy is important for security and virus protection.

***Automated Procurement Process**:* G-SI needs to reengineer the procurement process. Move away from the paper intensive procurement system in use today toward an automated on-line system. This promises to yield reduced procurement lead times and lessen the administrative workload. It will also increase contractor competition through more thorough dissemination of solicitation information.

***User Pull**:* User pull of information is needed. The field commander knows what information he needs. He needs the capability to pull data from the source, at his convenience, when it is needed and without intervention.

User Pull is needed to get the "right information at the right time" without overloading the user.

***Imagery**:* Operating Units need to be able to send images back and forth. The infrastructure for 210s and above should be built so this can occur.

There is an imagery requirement for emergency response situations, such as oil spills. The Intelligence Program also has a need to employ digitized imagery systems to enhance and extend tactical collection and use of intelligence.

3.3.11 G-WK (Medical)

***Consolidated Data Processing/Entry**:* They want one "box" (one system) for on-line entry and processing of data.

***Bandwidth Increase**:* The Composite Health Care System (CHCS) is used by DoD medical facilities to manage medical activity. Originally designed as an inpatient hospital data base, the system now has several management applications including supply, outpatient pharmacy, and outpatient clinic management (scheduling).

Under TRICARE agreements, telecommunications will be needed at Coast Guard medical facilities for connection to CHCS at all Coast Guard clinics. Adequate bandwidth will be needed. (These are DoD networks and CHCS does not currently have any connection to Coast Guard data networks. However, ten clinics currently have CHCS terminals which provide some interlink to DoD facilities in their area. This improves appointment scheduling for referrals, provides the capability for returning lab and x-ray results, and pharmacy on-line drug interaction databases, etc.).

Increased Database Capability: Forms need to be added to the database (medical, dental, patient history, etc.).

Automated Records Management: There is a requirement to digitize medical records. Medical records need to be kept and accessed electronically. (Anticipate 56k/pg. for imaging a standard medical form, and approximately 85k/pg. for an Officer Evaluation Report (OER).) The estimates are for image transmission. Character only transmission is much less bandwidth intensive.

Interoperability: Links with DoD are needed. DoD interlinks are required in support of the TRICARE system. Under TRICARE, the Coast Guard and DoD will be linked together into several medical "areas." DoD will provide the link.

Data Security: In the future, Coast Guard personnel may be permitted to enter some of their own medical data into the system. However, access should be limited and system security protection will be required. This capability would only exist at the unit via a CGSW III.

Automated Reporting System: A better way is needed to track medical treatment for Coast Guard personnel.

Imagery: The Navy is now successfully using telemedicine, including voice, data, and imagery, on shipboard and at remote locations for diagnosis and treatment. It is proving to be a very cost effective application despite the high bandwidth requirement and capital cost. At a minimum, the Program Manager desires the capability to electronically transmit pictures, such as medical records and radiology reports. This will be a large bandwidth requirement.

Maintain Clinic Automated Management System (CLAMS): There is a requirement to maintain current CLAMS capabilities, not necessarily the CLAMS system.

New Medical Expenses and Performance Reporting System (MEPRS): MEPRS data is recorded in the CLAMS with each patient visit. MEPRS is the means for billing Coast Guard beneficiaries' visits to DoD facilities and vice versa. CLAMS 2.0 will improve, but not replace, MEPRS by adding Current Procedural Terminology (CPT) and International Classification of Disease (ICD9) codes in addition to MEPRS codes. MEPRS codes will continue in use as long as DoD requires them. Coding is done manually. An automated system is under development .

***FAX-back**:* There are some requirements for documents (medical records, reports, forms, etc.) and other medical information to be passed back and forth via facsimile.

3.3.12 G-WP/WT (Personnel and Training)

***Bandwidth On Demand**:* Bandwidth on demand is needed to meet rapidly changing user requirements. For example, in the future, all personnel and medical data will be located at OSC Martinsburg. Additional bandwidth will be needed when all units have the capability to access this information. Personnel Management Information System (PMIS) and other administrative data bases are already combined into one central database, and Personnel Reporting Units (PERSRUs) may be eliminated as applications are pushed back to the operating units. Bandwidth requirements will increase even more when computer-based training delivers text and pictures to remote units, and audio and video capabilities are brought to each desk top. (This may ultimately yield a significant savings in the Coast Guard's travel budget.)

***Bandwidth Increase**:* Expanded user access, to a more robust Human Resources Database, will drive the need for increased bandwidth on the data network. Other administrative data requirements, such as just-in-time training and training-on-demand, will stretch the data network beyond the limit of its current capabilities.

***Scaleability**:* The network should be "scaleable" so that it can be quickly sized to meet rapidly changing user needs.

The current network does not meet user requirements. AR&SC's move to their own network is an example of a dissatisfied user. Program Managers know what service they want. The future network must be flexible and scaleable.

***Centralized Database**:* To realize a large savings in personnel costs, large data servers should be installed at OSC Martinsburg which will provide access at one location, with one-time entry, for all data.

All personnel and medical data will be located at OSC Martinsburg. They need the capability for all units in the Coast Guard to access this information.

***INTERNET Access for Every Coast Guard Member**:* Convert the current training system to a computer based training system (i.e., CD ROM, INTRANET, or INTERNET). If CD ROM is used, equipment purchase costs will be high. INTERNET appears to be the answer. Text and pictures are what they will deliver. There should be no Law Enforcement or other privacy/sensitive subject matter training on the INTERNET for security reasons. Subjects like Aids to Navigation, Personnel Management, or Communications training will be acceptable. The Coast Guard may elect to take advantage of the services provided by the INTERNET to reduce costs, unless some security requirements prohibit this.

Training needs access on the INTERNET for every unit in the Coast Guard. INTERNET access to non-sensitive information should save costs and provide easy access from member's terminals at work or at home. Once you get the INTERNET to the unit, the unit's Local Area Network (LAN) will provide access to each user. For training, users need to have 100% access.

Users need to have access to the INTERNET from home. This may yield an increase in productivity. It will also permit members to use terminal capabilities to the maximum extent possible.

***INTRANET**:* The Coast Guard needs an INTRANET which will use the same tools (WEB browser type interface) as the INTERNET. It will allow units access to various types of personnel management information, such as training quotas and records, and also to Coast Guard publications and directives. In designing the INTRANET, we need to make it easy for users to operate, or they won't use it.

User Charge Back: Users should pay for the services they use. Metered service equals a well informed user, and most importantly, it will help ensure that you never fall behind in meeting user requirements. User chargeback is very important and must be built in to any system. Users must pay for what they use to help keep network usage under control.

***Desktop Training Hardware**:* Audio and video capabilities at each desktop. Some organizations are already doing it. This would ensure the delivery of training to every member. If this is not feasible, audio and video capabilities could be limited to the Group level and above.

***Access to Training Information from Unit or Home**:* There are 15,000 unit training quotas in the system. There are approximately 15,000 more quotas not captured. There are obviously opportunities to manage the system better. Computer based training will produce a large savings. With it, members will be able to train at the unit or even at home.

***Automated Resource Allocation System**:* A better system is needed for evaluation and measurement of resource allocation.

3.4 Aggregate Requirements By Mission Area

This next step in the aggregation process is to organize and fine-tune the requirements under applicable missions. In the interest of consistency, we have used the same missions reported in the USCG C4I Baseline Architecture of 14 June 1996. (Note: We have added two other support programs not covered in the C4I Study.) In some cases, programs have estimated their future data communications requirements. A synopsis of those studies are included in appropriate sub-sections below. These studies will also be used to identify the gaps between future requirements and the current telecommunications baseline.

General Requirements:

The requirements listed below are considered "general" requirements spanning all Programs, and were discussed in nearly every one of the interviews. Each Program Manager Staff has some needs related to this list.

Network of Networks: A network capable of handling rapidly increasing demands for access to critical data and to meet speed of service requirements. Implement a network with sufficient bandwidth to cover current and future requirements. Also, provide the capability of obtaining additional bandwidth on demand, when surge capacity is needed.

Make the network flexible and scaleable enough to rapidly adjust to increasing or decreasing user requirements. Driving your automobile on an inter-state highway, requires you to adjust your speed based on highway conditions and traffic load. During heavy traffic conditions, if an additional High Occupancy Vehicle lane could be added to reduce the traffic load, the automobiles would be able to keep their speed at the desired level. Similarly, if the traffic load is light, lanes could be removed without affecting throughput. The same requirement exists for driving on the information super-highway. The Coast Guard needs the information super-highway to expand and contract effectively and efficiently, to meet the traffic demand. This enables the network to meet surge operations requirements and periods of peak demand between customers and their information centers. All Programs are seeking network services that provide inexpensive, reliable, and efficient communications.

Figures 3-2 and 3-3 present a user's perspective of the network of the future. Users will use one telephone to meet all voice requirements and one workstation to meet all data and video needs. The network itself will be transparent to the user who will be connected to the network by an intelligent gateway. The gateway will automatically select the best path from originator to addressee, depending on the type of service (i.e., voice telephone calls, record message traffic, applications, etc.) and based on whether the call is a voice, data, or video transmission. The network-of-networks is the vision of the future (10-15 years). Technology is not currently available to implement all aspects of this all-encompassing networking solution. However, technology is in place and will be in place in the next 5 years to implement significant portions of this vision.

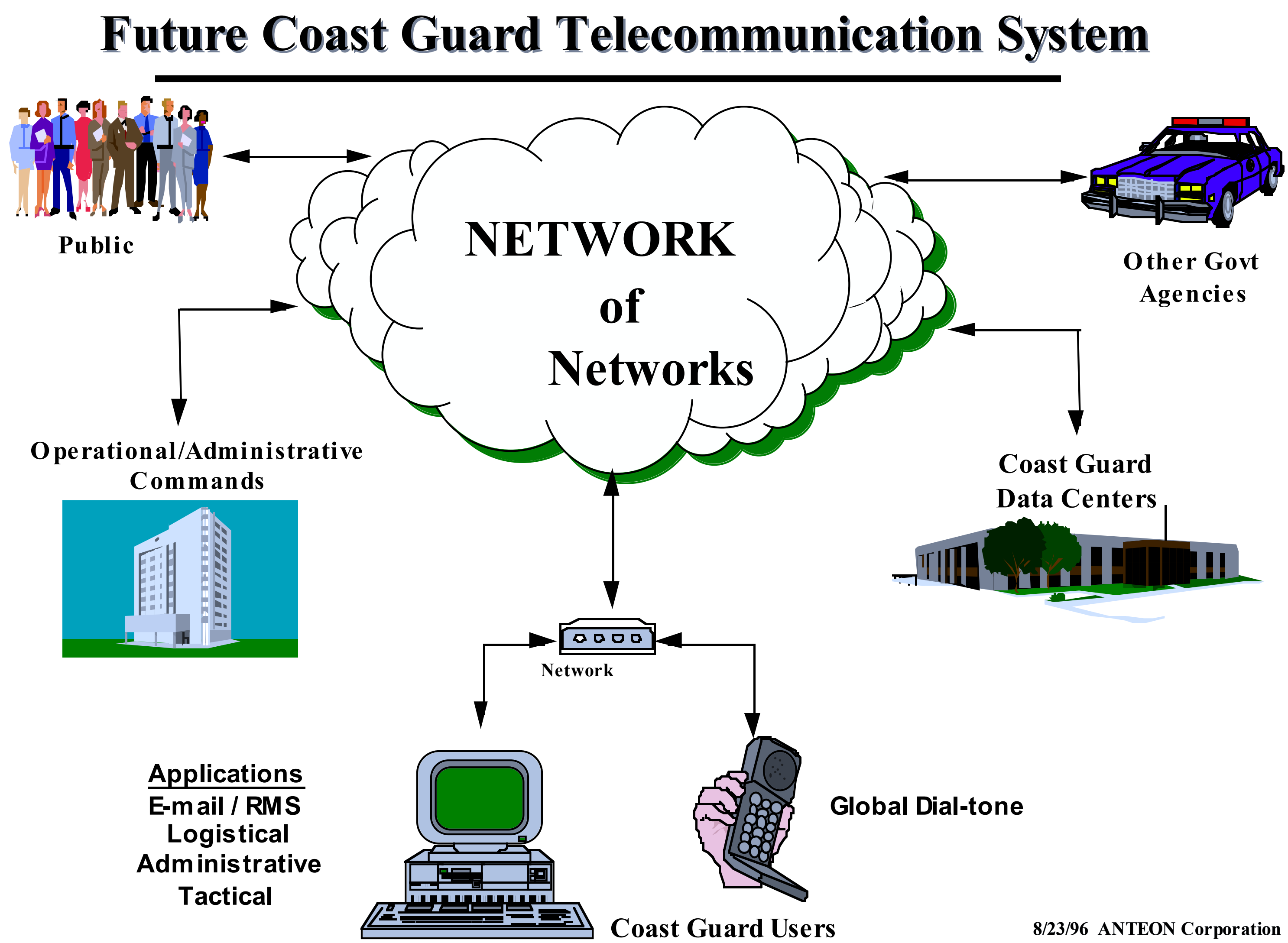


Figure 3-2: Network of Networks

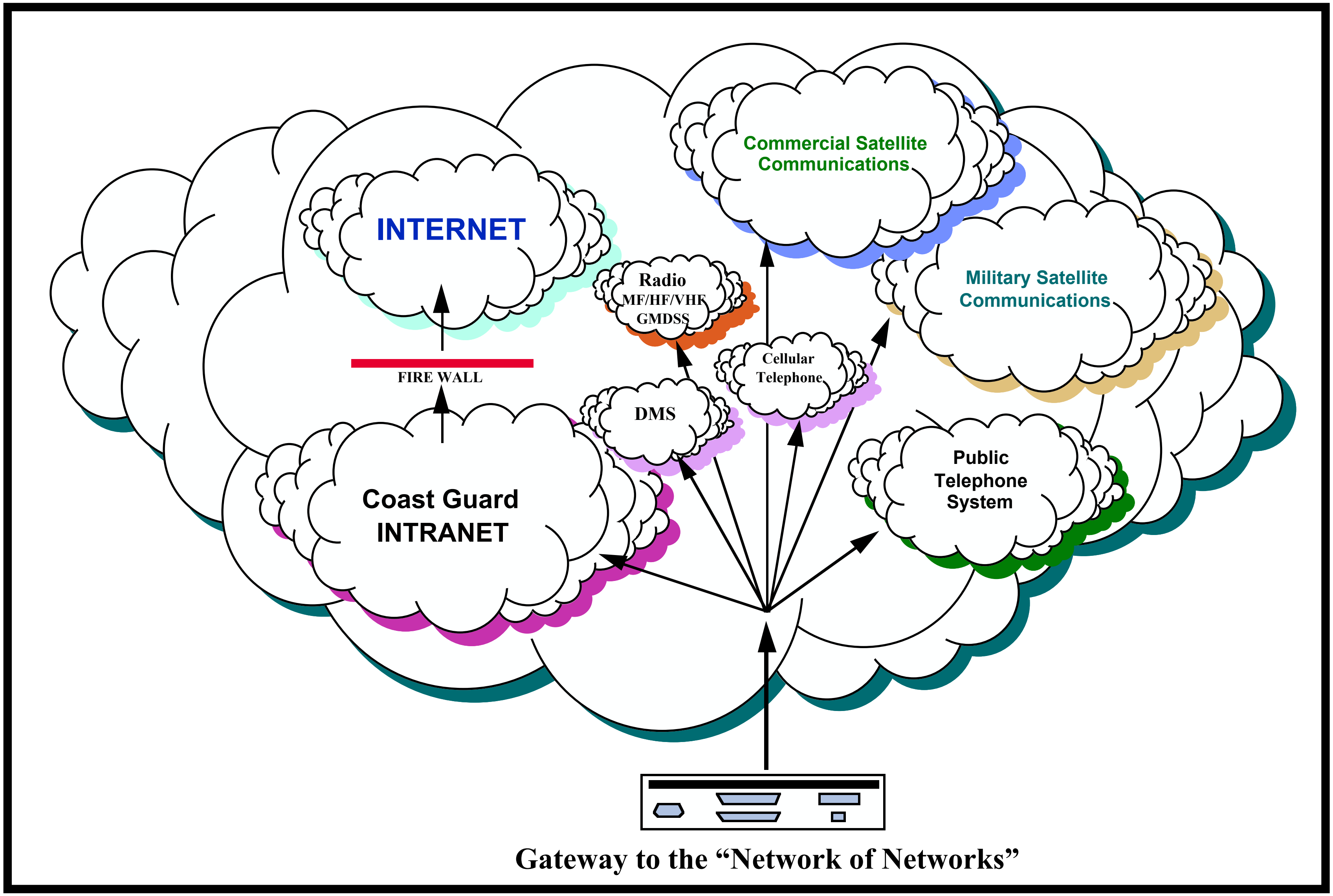


Figure 3-3: Intelligent Gateway Network Access

Formal and Informal Message Delivery: All Coast Guard units need some level of formal and informal message delivery capabilities. The future Defense Message System (DMS), used in conjunction with some form of electronic mail, may meet this requirement. Ships, in particular, need state-of-the-art messaging capabilities and need to fit in smoothly to the future network plan. Ships also have an increasing need for more "near real-time" data.

Automated Systems/One-Time Data Entry: "Automatic Information" is needed. This means that data submissions, where information is summarized and reported for SAR cases, special operations, floods, disasters, fuel/provisioning logistics information, etc., should be prepared only once, transmitted, received, logged, and displayed automatically without human intervention. For instance, aircraft need the capability to automatically broadcast flight information (hours flown, etc.) to all concerned. An Operations Information System (OIS)-type system may help meet this requirement.

The Programs have asked for one-time data entry 100% of the time.

There are other needs for automated systems. These include an on-line, fully integrated finance and procurement information system, and a centralized property tracking system with on-line query capability. Also included is the requirement for a common tactical picture (video clips) which is needed to meet mission status and situation reporting requirements in a multi-unit environment.

Centralized Data Storage and Access: Access by all units to all data at central locations via a WAN. Access should be available in "real-time" and "near real-time" depending on the user's requirement. This includes a "combined" database for operational information accessible by many organizational levels. Also included is a "combined" database for operational information accessible by many organizational levels.

Data Security: Limited access, secure and protected systems, and ease of use are required in the same environment. Multi-level security is needed to merge unclassified and classified traffic onto one terminal (e.g., marry the Secret-high LAN in both Areas with SIPRNET).

Remote Access: Remote access capabilities are needed (i.e., dial-up system that can be access from various locations (TAD, after hours from home, etc.)).

World-wide Access to Critical Internal Coast Guard Databases/Applications: This is where the bulk of Coast Guard business is conducted. INTRANETmay help meet this requirement.

Open Systems Architecture: Users of the future communication system need the capability of passing information anywhere, anytime. Systems must efficiently interact with each other.

Video and Imagery: Requirements for video and imagery are increasing across all Programs as the technology improves. These include sensor downloads from cutters and aircraft, still picture transmission, video clips from on scene, national intelligence information, etc.

User Pull: Users want to do their own driving on the information highway. They would like to have more control over the movement of data, and would prefer to have the capability to "pull" information, when they need it or when it is convenient for them to receive it, instead of having information "pushed" at them.

Global Dial-Tone: Users will have the capability to communicate with anyone, anytime using their single workstation (for all data needs) or telephone (for all voice communications).

In Sections 3.4.1 through 3.4.16, requirements that do not have application to all Coast Guard mission areas are listed by mission. An explanation of the requirement is included, where appropriate.

3.4.1 WWM/ATON (Waterways Management and Aids to Navigation)

Mobile Communications: Affordable and reliable communications bandwidth, to all Coast Guard mobile units, is needed. The use of state-of-the-art satellite technology (i.e., military and/or commercial) may result in improved communications services between shore units, cutters, and aircraft. Satellite services usually provide a faster and more reliable link than traditional methods of radio communications (i.e., MF, HF, or VHF).

World-wide Public Access to Coast Guard Information: NAVCEN may become the public INTERNET interface to Coast Guard databases. The public will have limited access to database information. This will require some paring down of the master on-line databases to yield information suitable for public access.

Interoperability: Fixed and mobile Coast Guard units need the ability to interface and communicate directly with OGAs. A gateway is needed, at a "fusion" site, for satellite communication interoperability.

Automated Chart Updates: Cutters need automated chart update capabilities while underway for safety of navigation purposes. There are numerous standards pertaining to programs for transmitting information of this type. The telecommunication system will be tapped to accommodate this. It needs to be reliable. There is a future requirement to update charts by data burst via the telecommunication system. They are updated manually now. NAVCEN may be assigned the responsibility of transmitting the updates.

Provide Navigation Information Service: NAVCEN is tasked with gathering, processing, and disseminating timely information to a wide variety of users. There is a requirement to maintain up-to-date technologies in dealing with their client base.

Solution to Cutter Antenna Interference Problems: There is a requirement to fix antenna interference problems on cutters. The problem is too many antennas, too little space. Increased mission requirements, over the years, have created a much greater demand on cutter communications capabilities than ever before. These demands have brought with them an increased inventory of communications equipment, including a myriad of antennas to handle several diverse modes of operation. Close proximity of transmitting and receiving antennas may result in varying levels of interference. The technology assessment will further investigate this issue.

3.4.2 SAR (Search and Rescue)

Mobile Communications: Affordable and reliable communications bandwidth, to all Coast Guard mobile units, is needed. Satellite communications may be the best solution to meet the ever increasing requirement for improved communications between cutters and aircraft. More tactical and situational information is needed on mobile units. A more effective interface is needed for exchanging information between larger Coast Guard platforms, that support the SAR mission, and shore facilities (Districts and Groups) and smaller platforms (WPBs and small boats). Identify a better, cheaper, faster alternative to INMARSAT.

Short Range Radio Communications: Ability to receive distress calls from all U.S. coastal areas where the majority of commercial or recreational vessel traffic exists. Comply with GMDSS requirements.

Automated Chart Updates: Cutters need automated chart update capabilities while underway for safety of navigation purposes. There are numerous standards pertaining to programs for transmitting information of this type. The telecommunication system will be tapped to accommodate this. It needs to be reliable. There is a future requirement to update charts by data burst via the telecommunication system. They are updated manually now. NAVCEN may be assigned the responsibility of transmitting the updates.

Interoperability: Fixed and mobile Coast Guard units need the ability to interface and communicate directly with OGAs and the public.

Direction Finding Capabilities: Direction finding capabilities are needed in the NDS.

Solution to Cutter Antenna Interference Problems: There is a requirement to fix antenna interference problems on cutters. The problem is too many antennas, too little space. Increased mission requirements, over the years, have created a much greater demand on cutter communications capabilities than ever before. These demands have brought with them an increased inventory of communications equipment, including a myriad of antennas to handle several diverse modes of operation. Close proximity of transmitting and receiving antennas may result in varying levels of interference. The technology assessment will further investigate this issue.

3.4.3 IO/MSA (Ice Operations and Marine Science Activities)

Mobile Communications: Affordable and reliable communications bandwidth, to Coast Guard mobile units, is needed. Satellite communications may be the best solution to meet the ever increasing requirement for improved communications between cutters and aircraft. Icebreakers need to effectively and reliably communicate or exchange data on a continuous basis from the polar regions with CONUS based facilities.

Automated Chart Updates: Cutters need automated chart update capabilities while underway for safety of navigation purposes. There are numerous standards pertaining to programs for transmitting information of this type. The telecommunication system will be tapped to accommodate this. It needs to be reliable. There is a future requirement to update charts by data burst via the telecommunication system. They are updated manually now. NAVCEN may be assigned the responsibility of transmitting the updates.

Interoperability: Fixed and mobile Coast Guard units need the ability to interface and communicate directly with OGAs.

Solution to Cutter Antenna Interference Problems: There is a requirement to fix antenna interference problems on cutters. The problem is too many antennas, too little space. Increased mission requirements, over the years, have created a much greater demand on cutter communications capabilities than ever before. These demands have brought with them an increased inventory of communications equipment, including a myriad of antennas to handle several diverse modes of operation. Close proximity of transmitting and receiving antennas may result in varying levels of interference. The technology assessment will further investigate this issue.

3.4.4 CVS (Commercial Vessel Safety)

Interoperability: Fixed and mobile Coast Guard units need the ability to interface and communicate directly with OGAs.

3.4.5 MEP (Marine Environmental Protection)

Mobile Communications: Affordable and reliable communications bandwidth, to all Coast Guard mobile units, is needed. Satellite communications may be the best solution to meet the ever increasing requirement for improved communications between cutters and aircraft. MEP units need the capability to communicate with small boats on VHF-FM during oil spills, etc.

Interoperability: Fixed and mobile Coast Guard units need the ability to interface and communicate directly with OGAs, including all public and private entities responding during environmental missions and emergencies.

Automated Chart Updates: Cutters need automated chart update capabilities while underway for safety of navigation purposes. There are numerous standards pertaining to programs for transmitting information of this type. The telecommunication system will be tapped to accommodate this. It needs to be reliable. There is a future requirement to update charts by data burst via the telecommunication system. They are updated manually now. NAVCEN may be assigned the responsibility of transmitting the updates.

3.4.6 PSS (Port Safety and Security)

Mobile Communications: Affordable and reliable communications bandwidth, to all Coast Guard mobile units, is needed. Satellite communications may be the best solution to meet the ever increasing requirement for improved communications between cutters and aircraft. PSS units need the capability to communicate with small boats on VHF-FM during operations, etc.

Interoperability: Fixed and mobile Coast Guard units need the ability to interface and communicate directly with OGAs.

3.4.7 ELT/MLE (Enforcement of Laws and Treaties/Maritime Law Enforcement)

Mobile Communications: Affordable and reliable communications bandwidth, to all Coast Guard mobile units, is needed. Satellite communications may be the best solution to meet the ever increasing requirement for improved communications between cutters and aircraft.

Automated Chart Updates: Cutters need automated chart update capabilities while underway for safety of navigation purposes. There are numerous standards pertaining to programs for transmitting information of this type. The telecommunication system will be tapped to accommodate this. It needs to be reliable. There is a future requirement to update charts by data burst via the telecommunication system. They are updated manually now. NAVCEN may be assigned the responsibility of transmitting the updates.

Interoperability: Fixed and mobile Coast Guard units need the ability to interface and communicate directly with OGAs.

Direction Finding Capabilities: Direction finding capabilities are needed in the NDS.

Solution to Cutter Antenna Interference Problems: There is a requirement to fix antenna interference problems on cutters. The problem is too many antennas, too little space. Increased mission requirements, over the years, have created a much greater demand on cutter communications capabilities than ever before. These demands have brought with them an increased inventory of communications equipment, including a myriad of antennas to handle several diverse modes of operation. Close proximity of transmitting and receiving antennas may result in varying levels of interference. The technology assessment will further investigate this issue.

3.4.8 CP/DO (Contingency Preparedness/Defense Operations)

Mobile Communications: Affordable and reliable communications bandwidth, to all Coast Guard mobile units, is needed. Satellite communications may be the best solution to meet the ever increasing requirement for improved communications between cutters and aircraft.

Interoperability: Fixed and mobile Coast Guard units need the ability to interface and communicate directly with OGAs.

Automated Chart Updates: Cutters need automated chart update capabilities while underway for safety of navigation purposes. There are numerous standards pertaining to programs for transmitting information of this type. The telecommunication system will be tapped to accommodate this. It needs to be reliable. There is a future requirement to update charts by data burst via the telecommunication system. They are updated manually now. NAVCEN may be assigned the responsibility of transmitting the updates.

Solution to Cutter Antenna Interference Problems: There is a requirement to fix antenna interference problems on cutters. The problem is too many antennas, too little space. Increased mission requirements, over the years, have created a much greater demand on cutter communications capabilities than ever before. These demands have brought with them an increased inventory of communications equipment, including a myriad of antennas to handle several diverse modes of operation. Close proximity of transmitting and receiving antennas may result in varying levels of interference. The technology assessment will further investigate this issue.

3.4.9 RBS (Recreational Boating Safety)

Interoperability: Fixed and mobile Coast Guard units need the ability to interface and communicate directly with OGAs.

3.4.10 Intelligence

Mobile Communications: Affordable and reliable communications bandwidth, to all Coast Guard mobile units, is needed. High speed communications is needed to cutters, aircraft, MSOs, etc. Satellite communications may be the best solution to meet the ever increasing requirement for improved communications between cutters and aircraft. Almost all networks are using TCP/IP, or are going to TCP/IP. With this in mind, determine how data will get to the ships. A larger pipe will be needed.

Interoperability: Fixed and mobile Coast Guard units need the ability to interface and communicate directly with OGAs.

***Telecommunications Support*:** Provide increased telecommunications support for Law Enforcement Detachments (LEDETs) and other field intelligence units. More needs to be done to provide operational intelligence support to the field.

3.4.11 Logistics (Fleet)

Mobile Communications: The requirement is to "move data." There is a need for efficient and reliable data communications with mobile units. Mobile units need the ability to effectively coordinate logistics support while underway.

On-Line Access: Access to the FAR must be included in the FLS.

Digital Signature Standard: There is a need to go to a digital signature standard.

3.4.12 Logistics (Aviation)

Digital Signature Standard: There is a need to go to a digital signature standard.

3.4.13 Personnel

Computer Based Training System: Convert the current training system to a computer based training system (i.e., CD ROM, INTRANET, or INTERNET).

User Charge-Back: Users should be charged for the services they use to help ensure that you never fall behind in meeting user requirements and to keep control of network usage.

3.4.14 Health & Safety

Interoperability: Links with DoD are needed.

TeleMedicine Capability: The capability is needed to electronically transmit pictures, such as medical records radiology reports, X-ray images, etc. (This requirement may be met through the use of imagery.)

3.4.15 Finance and Contracts

Real-Time Database Access: Units need to have access to real-time budget and expenditure data.

One-Time Data Entry: One-time data entry 100% of the time.

Digital Signature Standard: There is a need to go to a digital signature standard.

Consolidated Management Reporting System: This is a database used to keep the Commandant current on how well the Coast Guard is functioning.

Video Teleconferencing: Video teleconferencing capabilities are needed. This is the best substitute for actual face-to-face meetings and will save travel costs.

3.4.16 Legal

Automated Systems: G-L needs the capability to electronically transfer documents, such as case files, research data, etc.

3.5 Summary Table of All Requirements by Mission and Communications Criteria

Table 3-2 addresses the high level future requirements by mission as provided by the Program Managers. Each of the requirements is also categorized by criteria: voice, data, and video. For each stated need there is an estimate of the priority it carries within the mission area. We represented this by: H (high priority), M (medium priority), L (low priority). Also shown, are counts of Low, Medium, and High priorities for each column and row (mission and requirement). In addition, we have included weighted totals for each mission and requirement (H=5, M=3, L=1), and overall totals of all program and mission weighted values, including average, mean, mode, standard deviation, possible range, and high and low total values. This information should be useful to assess the overall value of each requirement and to ensure the mission mix and weighting is in line with overall Coast Guard grand and business strategy.

Table 3-2: Requirements By Mission

REQUIREMENTS	WWM/ATON	SAR	IO/MSA	CVS	MEP	PSS	ELT/MLE	CP/DO	RBS	Intel	Logistics (Fleet)	Logistics (Aviation)	Personnel & Training	Health & Safety	Finance & Contracts	Legal
Automated Systems/One Time Data Entry	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
NETWORK of Networks	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
Formal and Informal Message Delivery	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	M
Centralized Data Storage and Access	H	H	M	H	H	H	H	M	M	M	H	H	H	H	H	H
Data Security	M	H	M	H	H	H	H	M	H	H	M	M	H	H	H	H
Video & Imagery	H	H	H	H	H	H	H	H	M	H	H	L	L	H	M	M
Interoperability	M	H	H	H	H	H	H	H	H	H	M	M	M	H	L	L
Remote Access (Dial-In)	M	M	M	H	H	H	H	M	M	M	H	H	H	M	M	M
Worldwide internal access to Critical CG DB & Applications	M	M	M	M	H	H	H	M	M	M	M	M	H	M	M	H
Mobile Communications	H	H	H	H	H	H	H	H	H	M	L	L	L	L	L	L
Automated Chart Updates	H	H	H	L	H	H	H	H	M	H	L	L	L	L	L	L
World-wide Public Access to Coast Guard Databases	M	M	M	M	M	M	L	M	M	L	M	M	H	H	M	H
Provide Navigation Information Service	H	H	H	L	H	H	H	H	L	H	L	L	L	L	L	L
Short Range Radio Communications	H	H	M	L	H	H	H	M	H	M	L	L	L	L	L	L
Satellite Communications	H	H	H	L	M	M	H	L	L	M	H	L	L	L	L	L
Solution to Cutter Antenna Interference Problem	H	H	H	L	M	M	H	H	L	L	M	L	L	L	L	L
User Pull	M	L	M	L	M	L	M	L	L	L	M	M	M	M	M	M
Consolidated Management Reporting System	M	L	L	M	L	M	L	L	L	L	M	M	L	M	H	L
Direction Finding Capabilities	L	H	L	L	L	L	H	H	H	L	L	L	L	L	L	L
Video Teleconferencing	L	L	M	L	M	M	L	L	L	L	L	H	H	M	L	L
Telecommuting	L	L	L	H	L	M	L	L	L	L	L	H	L	L	M	M
Open Systems Architecture	H	L	L	L	M	M	L	L	L	L	L	L	L	L	L	L
Digital Signature Standard	L	L	L	L	L	L	L	L	L	L	M	M	L	L	M	L
Telemedicine Capability	L	L	L	L	L	L	L	L	L	L	L	L	L	H	L	L
User Charge Back	L	L	L	L	L	L	L	L	L	L	L	L	H	L	L	L
Global Dial-Tone	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L

Priorities: H=High, M=Medium, L=Low

Categories: d=Data, vi=Video, vo=Voice

3.6 Requirements Definitions

This section contains a brief definition of each of the requirements listed in Table 3-2 above. As each of these requirements relates to one or more of the critical gaps listed in Section 3.7, reference is made to the gap which most closely relates to the requirement. The critical gaps, in Section 3.7, directly relate to gaps identified in the C4I Baseline Architecture Document.

Currently, both the Telecommunications Plan and the C4I Baseline Architecture and Plan are in the process of development. These two efforts are related in many areas, and synergy can be obtained by ensuring these efforts are completed hand-in-hand. Significant input, to the development and preparation of the Program Manager Interview questions, was obtained from drafts of the C4I Baseline Architecture document. The C4I document identified critical gaps in capabilities. These gaps correlate directly to many of the future requirements addressed in the

Telecommunications Plan. The focus of the Telecommunications Plan differs from the C4I Baseline Architecture in that it is limited to communications requirements, but it addresses these requirements throughout the Coast Guard. Accordingly, the Telecommunications Plan incorporates several programs not addressed by the C4I efforts, particularly administrative and support. For this reason, not all requirements, in the Telecommunications Plan, will link directly to the critical gaps discussed in the C4I documents.

- **Network of Networks:** Network of the future; transparent to the user; meets all user requirements. A flexible and scaleable network capable of efficiently handling the rapidly increasing demands for access to critical data while meeting speed of service/bandwidth requirements. Meets all current and future voice, data, and video requirements. (All Gaps)

- **Formal and Informal Message Delivery:** Delivery of record message traffic and electronic mail anywhere, anytime. (Gap: Communications Connectivity)

- **Automated Systems/One Time Delivery of Data:** Data submissions, where information is summarized and reported for SAR cases, special operations, floods, disasters, fuel/provisioning logistics information, etc., should be prepared only once, transmitted, received, logged, and displayed automatically without human intervention. (Gap: Information Exchange)

- **Centralized Data Storage and Access:** The ability for automated systems to access data that is stored and maintained in one location. (Gap: Information Exchange)

- **Data Security:** Protection of sensitive and/or classified information from unauthorized access. Multi-level security is needed to merge unclassified and classified traffic onto one terminal. (Gap: Data Security)

- **Interoperability:** The ability for fixed and mobile Coast Guard units to interface and communicate directly with other government agencies. (Gap: Interoperability)

- **Remote Access (Dial-in):** Ability for users to access information by dialing into systems over the public telephone system by means of a modem. (Gap: Communications Connectivity and Information Exchange)

- **World-wide Public Access to Coast Guard Databases:** Ability for the public to access information, that is made available to them by the Coast Guard, from anywhere in the world. (Gap: Information Exchange)

- **Video & Imagery:** The transmission of moving frames or pictures of information. (Gap: C3 Systems and Decision/Tactical Support)

- **<u>Mobile Communications:</u>** Affordable and reliable communications bandwidth to Coast Guard mobile units is needed. The need for improved communications between cutters and aircraft is critical. (Gap: Communications Connectivity)

- **<u>World-wide Internal Access to Critical CG Database Applications:</u>** Ability for Coast Guard users to access Coast Guard databases and applications from anywhere in the world (i.e., INTERNET/INTRANET access, dial-in modem, etc.). (Gap: Information Exchange)

- **<u>Provide Navigation Information Service:</u>** Provide easy-access to navigational information for Coast Guard personnel and the public by means of voice systems or a data repository (e.g., INTERNET, etc.). (Gap: Maritime Public Support)

- **<u>Short Range Radio Communications:</u>** High speed, reliable communications connectivity between all levels of operational units and the maritime public. Ability to receive distress calls from all U.S. coastal areas where commercial or recreational vessel traffic exists. Comply with Global Maritime Distress and Safety System (GMDSS) requirements. (Gap: Communications Connectivity)

- **<u>Automated Chart Updates:</u>** Cutters need automated chart update capabilities while underway. There are numerous standards pertaining to programs for transmitting information of this type. There is a future requirement to update charts by data burst via the telecommunication system. They are updated manually now. NAVCEN may be assigned the responsibility of transmitting the updates. (Gap: Information Exchange)

- **<u>Solution to Cutter Antenna Interference Problem:</u>** There is a requirement to fix antenna interference problems on cutters. The problem is too many antennas, too little space. Increased mission requirements, over the years, have created a much greater demand on cutter communications capabilities than ever before. These demands have brought with them an increased inventory of communications equipment, including a myriad of antennas to handle several diverse modes of operation. Close proximity of transmitting and receiving antennas may result in varying levels of interference. The technology assessment will further investigate this issue. (Gap: Communications Connectivity and C3 Systems)

- **<u>Telecommuting:</u>** Ability for personnel to perform their job adequately from locations outside of their normal work location (i.e., dial-in access to all required databases and applications). (Gap: Communications Connectivity)

- **<u>Satellite Communications:</u>** Ability for mobile or shore units to communicate or transfer data by means of satellite technology. (Gap: Communications Connectivity)

- **<u>Direction Finding Capabilities:</u>** Determine the location of vessels in support of Coast Guard SAR and L/E missions. (Gap: Maritime Public Support)

- **<u>User Pull:</u>** Ability for authorized personnel to access and/or download data, such as message traffic, directives, and publications, for operational or administrative purposes. (Gap: Information Exchange)

- **<u>Video Teleconferencing:</u>** Ability for personnel to meet without the need for travel by transmitting video, voice, and data between video conferencing centers or workstations. (Gap: Decision/Tactical Support)

- **<u>Consolidated Management Reporting System:</u>** A database where operational and budget information are consolidated to provide a strategic Decision Support System for the Coast Guard. (Gap: Decision/Tactical Support)

- **<u>Digital Signature Standard:</u>** A standard needs to be developed that designates requirements for digital signatures for the purpose of establishing and guaranteeing authenticity of documents created electronically. (Gap: Information Exchange)

- **<u>Telemedicine Capability:</u>** A system that will provide medical personnel with the ability to perform medical transactions automatically. (Gap: Information Exchange)

- **<u>User Charge-back:</u>** Ability to accurately calculate system usage and to charge each user of a system for the services they have used. (Gap: Information Exchange)

- **<u>Global Dial-Tone:</u>** Ability to access a dial-tone world-wide for the purposes of calling anywhere, anytime for voice, data, or video needs. (Gap: Communications Connectivity)

- **<u>Open Systems Architecture:</u>** A model that represents a network as a hierarchical structure of layers of functions. Each layer provides a set of functions that can be accessed and used by the layer above it. (Gap: Information Exchange)

3.7 Gap Identification

In the previous sections, future communications requirements were identified by Program and Mission. These requirements have been compared to the Baseline Architecture in Chapter 2 of the Telecommunications Plan, and with the gaps identified in the C4I Baseline Architecture document. (Where there is a clear and direct relationship between the gaps below and the C4I Baseline Architecture document, reference is made to the specific page in the C4I document where the gap can be found.)

This section identifies the gaps between the Telecommunications Plan baseline architecture and the future requirements. This process establishes the framework for our assessment of relevant technologies and recommended solutions (Chapter 4). It will also indicate, where applicable, if a requirement has a clear and direct relationship to another publication or document (i.e., C4I Baseline Architecture Document, etc.).

The resulting list below shows the most critical gaps in Coast Guard communications capabilities.

- ***Communications Connectivity:*** The lack of high speed and reliable communications connectivity, including secure/protected communications, between all levels of operational units. This includes personnel in the field, boats, cutters, aircraft, and operational shore facilities that require, as a minimum, voice and data communications. The following are examples of critical gaps in communications connectivity, taken directly from the C4I Baseline Architecture document:

  - ♦ The inability to receive detailed and complex information from patrol assets, without much difficulty and manual labor. (C4I pg. 7-43)
  - ♦ The lack of reliable connectivity between cutters, aircraft, boats, and operational shore facilities, including at extended ranges. (C4I pg. 8-43)
  - ♦ The lack of a quick and efficient mechanism to advise units and personnel in the field of critical aids-to-navigation outages to facilitate the most effective use of Short-Range Aids-to-Navigation (SRA) resources. (C4I pg. 3-58)
  - ♦ The lack of a communications path to get ice surveillance information (satellite imagery or reconnaissance information from aircraft) to operational planners (Districts and Groups) and cutters. (C4I pg. 5-59)
  - ♦ The lack of the ability for the Officer-in-Charge, Marine Inspections (OCMI) to conduct effective communications with inspectors and investigators in the field, including the ability to exchange data (and imagery, if required) when the OCMI must make a decision on complex issues or command expertise is required by field personnel. (C4I pg. 6-35)
  - ♦ The lack of the ability for the Marine Safety Office (MSO)/On Scene Coordinator (OSC) to easily and effectively conduct communications throughout an assigned port and/or Captain of the Port (COTP) area, including effective communications with field personnel (including secure communications). (C4I pg. 7-43, 13-17)
  - ♦ The lack of the ability to conduct the robust communications, in all modes (voice, data, imagery, and secure) that are required between the OSC and personnel on-scene during critical operations, such as SAR, medical emergencies, natural disasters, pollution incidents, etc. (C4I pg. 7-43)

- ♦ The lack of the capability of the MSO/COTP to monitor vessel communications, particularly Bridge-to-Bridge communications, throughout the port/COTP area. (C4I pg. 8-43)

- ♦ The lack of reliable connectivity between cutters, aircraft, boats, and operational shore facilities, including at extended ranges.

- ♦ The lack of high speed and reliable communications between mobile assets (cutters, Aids to Navigation Team (ANT) boats and personnel in the field) and operational support information to assist in the execution of the SRA mission. (C4I pg. 3-59, 4-45, 9-53)

- ♦ As related to the Port State Control program, the limited ability of the OCMI to communicate with Coast Guard resources, commercial vessels and field personnel offshore. (C4I pg. 6-36)

- ♦ The lack of ability to conduct the robust communications, in all modes (voice, data, imagery, and secure) that are required between the OSC and personnel on scene at a pollution incident and/or between the OSC command center and a field command center at the scene of action. (C4I pg. 7-43)

- ♦ The lack of the ability for the MSO/COTP to easily and effectively conduct communications throughout an assigned port and/or COTP area, includes communications with field personnel (including secure communications). (C4I pg. 8-42)

- ♦ Standardization and interoperability with other Coast Guard systems. (C4I pg. 11-37)

- ♦ The lack of reliable communications connectivity, including secure/protected communications, between all levels of operational units. This includes personnel in the field, boats, cutters, aircraft and operational shore facilities that requires as a minimum voice and data communications. (C4I pg. 13-17)

- ***Maritime Public Support:*** The inability to effectively provide consistently reliable maritime public communications support at all times and in all areas.

  - ♦ The lack of the ability to receive all distress calls in some portions of U.S. coastal areas where the majority of commercial or recreational vessel traffic exists. (C4I pg. 4-44)

  - ♦ The limited communications capabilities available to support multiple situations, crises, and/or operations simultaneously. (C4I pg. 4-44)

- ♦ The inability to reduce communications on already crowded maritime mobile VHF-FM channels, and to communicate with vessels and pilots in an automated manner via data communications modes. (C4I pg. 3-58)

  The limited abilities to get the broad scope of recreational boating safety information to the public in an easy and cost efficient manner. (C4I pg. 11-37)

- ***Interoperability:*** The general lack of communications capabilities at Coast Guard operational units to effectively interface with other government agencies (e.g., federal, state, and local law enforcement agencies). Gaps include the following:

  - ♦ The limited capabilities available to Groups, Small Boat Stations, and other Coast Guard resources to interface effectively with the numerous federal, state, and local agencies that are involved in the execution of Coast Guard missions, such as SAR, ice operations, law enforcement, marine inspection, etc. (C4I pg. 4-44)

  - ♦ The lack of the ability for Groups and small boats to interface effectively with Navy and other DoD resources that may be assisting in the execution of Coast Guard missions. (C4I pg. 13-17)

  - ♦ In some situations, the limited capabilities available to Groups and cutters to interface effectively with the numerous federal, state, and local agencies that may be involved or concerned regarding ice conditions, vessel transits and icebreaking operations. (C4I pg. 5-59)

  - ♦ The limited capabilities of the OCMI and field inspectors/investigators to interface effectively with the numerous federal, state, and local agencies and private/commercial organizations concerned with commercial vessel safety. (C4I pg. 6-36)

  - ♦ The limited capabilities available to the OSC and Coast Guard resources to interface effectively with the numerous federal, state, and local agencies that may and are involved in the execution of the MEP mission and in responding to spills and other hazardous material situations. (C4I pg. 7-43)

  - ♦ The limited capabilities available to the COTP, Groups, Small Boat Stations and other Coast Guard resources to interface effectively with the numerous federal, state, and local agencies that may be involved in the execution of the PSS/ELT/MLE missions and port safety or security situations. (C4I pg. 8-43, 9-52)

  - ♦ The limited capabilities of Coast Guard assets that routinely interface with other federal assets to exchange information. (C4I pg. 9-53)

- ♦ The lack of effective and reliable organizational interoperability between different classes of Coast Guard assets (cutters, aircraft, boats and operational shore facilities; Groups, MSOs, Commander of Coast Guard Forces (CCGFs) and Districts). (C4I pg. 10-55)

  The lack of the ability by Commander of Coast Guard Forces (CCGFs, Groups, MSOs and in come cases Small Boat Stations to effectively interface with other Government Agencies and Non-Government Organizations when a natural disaster or emergency occurs. The Coast Guard's standard suite of communications equipment may in many cases not prove sufficient to support required operations in disaster/emergency situations. Complicating the problem is that the communications suites and systems required may vary by geographic or operating area. (C4I pg. 10-55)

- ♦ The lack of the ability by Coast Guard assets to effectively interface with DoD assets, not only for Defense Operations, but also as related to Contingency Preparedness. DoD assets routinely respond to disasters or emergencies. These assets use DoD organic C4I and communications equipment and expect other agencies to be interoperable. (C4I pg. 10-55)

- ♦ The lack of the ability to interchange information easily and efficiently with state agencies responsible for recreational boating safety, enforcement and licensing/registration programs. (C4I pg. 11-37)

- ♦ The general lack of communication capabilities of Groups to effectively interface with other agencies throughout assigned AORs. Lack of effective communications with aircraft. (C4I pg. 13-17)

- ***<u>Information Exchange:</u>*** The lack of an effective interface for exchanging information between larger Coast Guard platforms that support the SAR mission and shore facilities (Districts and Groups) and smaller platforms (WPBs and small boats). This includes the lack of seamless interfaces for effective transmission of information between small boats, larger cutters, aircraft, and shore facilities. Of particular note is the lack of effective communications between ships and aircraft. The following are critical gaps in communications capability that may be solved by use of new and improved technology, such as the Operations Information System (OIS):

  - ♦ Inability of command and control units to readily access location, status, and capability information on subordinate units/resources.

  - ♦ The inability to effectively maintain situational awareness at District, Group, and MSO command centers. The inability to effectively use readily available information on board smaller cutters and small boats.

- ♦ The lack of an effective interface for exchanging information between larger Coast Guard platforms that support the SAR mission and shore facilities (Districts and Groups) and smaller platforms (WPBs and small boats). (C4I pg. 4-45)

- ♦ The lack of an effective interface for exchanging information between larger Coast Guard platforms that may support the MEP/PSS/ELT missions, shore facilities, and smaller platforms and personnel in the field, with the COTP Command Center. (C4I pg. 7-43, 8-43, 9-52)

- ♦ The lack of the ability to effectively exchange sensor, intelligence and other tactical information between aircraft, mobile units, and shore facilities. (C4I pg. 9-52)

- ♦ The lack of easy access of the field level to information on recreational boats, including ownership, licensing and registration information. (C4I pg. 11-37)

- ♦ The lack of timely access at operational units to critical personnel data. (C4I pg. 12-82)

- ♦ The lack of timely updates of personnel and entitlement information. (C4I pg. 12-82)

- ♦ The lack of common, easy to use and effective interfaces for transmission of information, including sensor data/information, between small boats, larger cutters, aircraft and shore facilities. (C4I pg. 13-17)

- ***Data Security:*** There is a general lack of ability to protect sensitive communications between SMCs and OSCs particularly in coastal areas where smaller Coast Guard resources/platforms are used.

- ***Decision/Tactical Support:*** There exists a general lack of effective decision/tactical support tools and systems on mobile units. State-of-the-art technology is needed to improve and enhance the overall conduct of mission operations. This includes the requirement for keeping operational commanders current on the status of on-going operations. A common tactical picture sent from the on-scene commander, over data transmission circuits, to the operational commander ashore is one viable solution.

- ***C3 Systems:*** The general cumbersome interfaces available for using Coast Guard Command and Control/Communication systems. Innovative telecommunications solutions are needed to fix the problem and fill the gap. Faster, more reliable and efficient interfaces are needed between large and small cutters, cutters and aircraft, and between cutters, aircraft, and shore units to meet all administrative and operational communications requirements. (C4I pg. 3-59, 4-44, 6-36, 7-43, 8-43, 9-53, 10-55)

3.8 Wide Area Network (WAN) Bandwidth Requirements

The previous sections have dealt with functional requirements and the gaps between them and the current telecommunications baseline. All of the requirements and gaps involve movement of data into, out of, and within the Coast Guard. Most of that movement requires a WAN with the ability to connect with all Coast Guard entities. One significant task is the determination of the volumes of data that must move concurrently on the circuits at any point in time. This problem has been compared to liquid transportation through pipelines. The data problem is sometimes referred to as "sizing the pipes." The whole process is important since the cost of the network is very much related to the "size of the pipes" to all Coast Guard personnel.

Different legs of the network may require different magnitudes of data flow. The requirements for a Coast Guard WAN are an accumulation of all the requirements from Coast Guard applications producing data for movement within the organization. There are only two program/application managers who have produced detailed quantified studies of their data communication requirements.

3.8.1 Current Telecommunications Capacity Requirements Studies

1. **Personnel Management Information System II (PMIS II):** The Preliminary Technical Alternatives and Cost Analysis Report was completed by Ogden Professional Services Corporation (now Anteon) in conjunction with Mnemonic Systems, Inc. and various elements of Coast Guard PMIS management. It was completed in February 1996. The conclusions of the study were three fold: the system should use a central database, served by a Sequent S5000 SE70 minicomputer and a Frame Relay service WAN.

   The data communications portion of the study was built from scratch. To do that, experts on the current system, involved with development of PMIS II, were tasked to estimate the size and frequency of all prospective PMIS II transactions. These were grouped according to similar units. The PMIS II data can be viewed in Table 3-3.

   A key measurement for peak system loading is the maximum number of bits per second required. This is estimated for each type of unit studied for PMIS II. The total peak bandwidth requirement is the Grand Total of all interactions with the host site (OSC Martinsburg). This total can only be reasonably expected at the host site, but the other capacities of the individual unit types are estimated by Table 3-3. To obtain a detailed analysis the individual application, bandwidth needs must be totaled for each leg of the network. Table 3-3 only represents PMIS II requirements for communications bandwidth. Presenting the total picture requires similar estimates from several other programs and applications within the Coast Guard.

2. **<u>Fleet Logistics System(FLS)</u>:** The other data communications survey is included in the FLS Technical Infrastructure Study (TIS) and the FLS Requirements Analysis (Final). Version 1.2 is dated September 20, 1996 and was produced by OAO Corporation for the Office of G-AFL. Some of its results are displayed in Table 3-4 (as modified by Anteon staff, see section on Data Validity). Again these figures only represent FLS requirements. Other programs and applications are estimated in Table 3-5 and a compilation is made there for OSC Martinsburg peak bandwidth.

3. **<u>Data Validity</u>:** The PMIS II study seems to hit closest to an expected result. From the documentation accompanying this study, a growth factor was not indicated as part of the estimation process. We have added a growth factor of 3 into the table which leads to our figures in Table 3-3.

4. **<u>Bandwidth Calculations:</u>** In the FLS study the bandwidth calculation used a formula that resulted in unusually high results. For instance the peak bandwidth numbers were 95 times those of PMIS II. We used the "character count" from the OAO study and developed another formula to estimate peak bandwidth. This new approach yielded FLS totals approximately one and one half times the PMIS data. PMIS II and FLS combine for an estimated peak capacity of 373 kbits/sec coming into the host site (OSC Martinsburg). This would occupy one-fourth of a T1 circuit (1544 kbits/sec). T1 is an important standard in communications and therefore is a key breakpoint and scale for costing networks.

5. **<u>What next?</u>** In Table 3-5 several very rough estimates for OSC Martinsburg bandwidth requirements are made for the applications/programs other than PMIS II and FLS. They are combined with the FLS and PMIS study estimates in Figure 3-5. This is a graphic representation of the cross section of the data pipe entering OSC Martinsburg. The estimates are extremely vulnerable to system architecture decisions and user acceptance of future systems. Improving the accuracy of the peak bandwidth requirements depends on the completion of similar studies for those other present and developing major applications within the Coast Guard.

   Conclusions that can be made about the overall peak bandwidth at the central site can be applied to the individual legs of the WAN for the applications with detailed studies. The tables should be geared to the individual site level, which will give the analyst the capability of figuring bandwidth on every required leg of the network

Table 3-3: Communications Circuit Estimates

PMIS II									
UNIT DESCRIPTION	**Site count**	**Peak concurrent users**	**Total Bytes (annual)**	**Avg load in Kbits/sec**	**Peak Load in Kbits/sec**	**Peak load plus 'Future Growth Factor'**	**Peak Kbits/sec per site**	**Total PMIS activity to site**	**Percent of T1 pipe to site**
large units	252	725							
to central DB			2,849,819,259	3.93	5.50	16.49	0.07		
fm central DB			8,657,443,293	11.93	16.70	50.10	0.20		
Sub total			11,507,262,552	15.86	22.20	66.59	0.26	1.23%	0.02%
small units	457	160							
to central DB			859,870,277	1.18	1.66	4.98	0.01		
fm central DB			8,013,053,484	11.04	15.46	46.37	0.10		
Sub total			8,872,923,761	12.23	17.12	51.35	0.11	0.52%	0.01%
HQ	1								
to central DB			145,181,112	0.20	0.28	0.84	0.84		
fm central DB			751,941,665	1.04	1.45	4.35	4.35		
Sub total			897,122,777	1.24	1.73	5.19	5.19	24.19%	0.34%
MPC	1								
to central DB			202,394,000	0.28	0.39	1.17	1.17		
fm central DB			248,736,825	0.34	0.48	1.44	1.44		
Sub total			451,130,825	0.62	0.87	2.61	2.61	12.16%	0.17%
PPC	1								
to central DB			134,517,150	0.19	0.26	0.78	0.78		
fm central DB			159,577,155	0.22	0.31	0.92	0.92		
Sub total			294,094,305	0.41	0.57	1.70	1.70	7.93%	0.11%
ISC's	12								
to central DB			274,637,088	0.38	0.53	1.59	0.13		
fm central DB			664,459,502	0.92	1.28	3.85	0.32		
Sub total			939,096,590	1.29	1.81	5.43	0.45	2.11%	0.03%
TraUnits	9								
to central DB			328,999,839	0.45	0.63	1.90	0.21		
fm central DB			567,252,803	0.78	1.09	3.28	0.36		
Sub total			896,252,642	1.23	1.73	5.19	0.58	2.68%	0.04%
Independent units	473								
to central DB			25,350,264	0.03	0.05	0.15	0.00		
fm central DB			7,119,179,209	9.81	13.73	41.20	0.09		
Sub total			7,144,529,473	9.84	13.78	41.35	0.09	0.41%	0.01%
External customers	1								
to central DB			181,445,000	0.25	0.35	1.05	1.05		
fm central DB			1,627,388,000	2.24	3.14	9.42	9.42		
Sub total			1,808,833,000	2.49	3.49	10.47	10.47	48.77%	0.68%
TOTAL		1976							
to central DB			5,002,213,989	0.69	9.65				
fm central DB			27,560,295,111	3.80	53.64				
Grand Total						**189.88**	**Kbits/sec**		
				Percent of one T-1		**12.30%**			
		Site count	=	Taken from PMIS study					
	Peak concurrent users		=	Taken from PMIS study					
	Total Bytes (annual)		=	Taken from PMIS study					
	Avg load in Kbits/second		=	Total Byes (annual)/ seconds per work year/ 1000					
	Peak load in Kbits/second		=	Avg load in Kbits/sec* PMIS average to peak users loading factor of 1.4					
Peak load plus 'Future Growth Factor'			=	Peak load in Kbits/sec* Growth Factor of 3					
	Peak Kbits/sec per site		=	PMIS average to peak users loading factor of 1.4/ Site count					
	Total PMIS activity to site		=	Peak Kbits/sec per site/ Peak Kbits/sec					
	Percent of T1 pipe to site		=	Peak Kbits/sec per site/ 1.544 Kbits per second (T1 speed)					

Table 3-4: Communications Circuit Estimates

FLS								
UNIT DESCRIPTION	**Count**	**Peak concurrent users**	**Total Bytes (per user per day)**	**Total Bytes (annual)**	**Peak load Kbits/sec**	**Peak load plus 'Future Growth Factor'**	**Total FLS activity to site**	**Percent of T1 pipe to site**
MAJOR SITES								
HQ		42	85000	899640000	4.96	14.88	5.26%	0.96%
ELC								
Supply Center Curtis Bay		120	85000	2570400000	14.17	42.50	15.02%	2.75%
Supply Center Baltimore		100	85000	2142000000	11.81	35.42	12.51%	2.29%
Coast Guard Yard		80	85000	1713600000	9.44	28.33	10.01%	1.84%
Warehouse Columbia MD		15	85000	321300000	1.77	5.31	1.88%	0.34%
MLCP Onsite		81	85000	1735020000	9.56	28.69	10.14%	1.86%
MLCA Onsite		207	85000	4433940000	24.44	73.31	25.90%	4.75%
sub-total (major sites)		645						
ISCs								
Alameda		3	25000	18900000	0.10	0.31	0.11%	0.02%
Boston		3	25000	18900000	0.10	0.31	0.11%	0.02%
Cleveland		3	25000	18900000	0.10	0.31	0.11%	0.02%
Honolulu		3	25000	18900000	0.10	0.31	0.11%	0.02%
Miami		3	25000	18900000	0.10	0.31	0.11%	0.02%
New Orleans		3	25000	18900000	0.10	0.31	0.11%	0.02%
New York		3	25000	18900000	0.10	0.31	0.11%	0.02%
Portsmouth		3	25000	18900000	0.10	0.31	0.11%	0.02%
Seattle		3	25000	18900000	0.10	0.31	0.11%	0.02%
St Louis		3	74000	55944000	0.31	0.93	0.33%	0.06%
NESUs								
Alameda		4	30000	30240000	0.17	0.50	0.18%	0.03%
Boston		5	30000	37800000	0.21	0.63	0.22%	0.04%
Cleveland		3	30000	22680000	0.13	0.38	0.13%	0.02%
Honolulu		3	30000	22680000	0.13	0.38	0.13%	0.02%
Miami		3	30000	22680000	0.13	0.38	0.13%	0.02%
New Orleans		5	30000	37800000	0.21	0.63	0.22%	0.04%
New York		3	30000	22680000	0.13	0.38	0.13%	0.02%
Portsmouth		9	30000	68040000	0.38	1.13	0.40%	0.07%
Sea/Star Ship Supply		13	30000	98280000	0.54	1.63	0.57%	0.11%
Seattle		6	30000	45360000	0.25	0.75	0.26%	0.05%
St Louis		7	30000	52920000	0.29	0.88	0.31%	0.06%
CG MRD								
Satellite Site		2	30000	15120000	0.08	0.25	0.09%	0.02%
River Tender								
MAT-St Louis		1	30000	7560000	0.04	0.13	0.04%	0.01%

Table 3-4: Communications Circuit Estimates (Cont.)

FLS								
UNIT DESCRIPTION	**Count**	**Peak concurrent users**	**Total Bytes (per user per day)**	**Total Bytes (annual)**	**Peak load Kbits/sec**	**Peak load plus 'Future Growth Factor'**	**Total FLS activity to site**	**Percent of T1 pipe to site**
Alameda		5	30000	37800000	0.21	0.63	0.22%	0.04%
New Bedford		2	30000	15120000	0.08	0.25	0.09%	0.02%
Boston		2	30000	15120000	0.08	0.25	0.09%	0.02%
Honolulu		2	30000	15120000	0.08	0.25	0.09%	0.02%
New York		2	30000	15120000	0.08	0.25	0.09%	0.02%
Portsmouth		6	30000	45360000	0.25	0.75	0.27%	0.05%
San Pedro		1	30000	7560000	0.04	0.13	0.04%	0.01%
EMD								
Boston		2	78000	39312000	0.22	0.65	0.23%	0.04%
Cleveland		2	42000	21168000	0.12	0.35	0.12%	0.02%
Miami		3	5000	3780000	0.02	0.06	0.02%	0.00%
New Orleans		2	42000	21168000	0.12	0.35	0.12%	0.02%
New York		3	42000	31752000	0.18	0.53	0.19%	0.03%
Portsmouth		3	42000	31752000	0.18	0.53	0.19%	0.03%
St. Louis		1	42000	10584000	0.06	0.18	0.06%	0.01%
ESUs								
Alameda		7	30000	52920000	0.29	0.88	0.31%	0.06%
Honolulu		5	30000	37800000	0.21	0.63	0.22%	0.04%
Kodiak		2	30000	15120000	0.08	0.25	0.09%	0.02%
Seattle		6	30000	45360000	0.25	0.75	0.27%	0.05%
Weapons Team								
Boston		3	33000	24948000	0.14	0.41	0.15%	0.03%
Key West		1	33000	8316000	0.05	0.14	0.05%	0.01%
Portsmouth		3	33000	24948000	0.14	0.41	0.15%	0.03%
270 MAT								
Key West		3	30000	22680000	0.13	0.38	0.13%	0.02%
St. Petersberg		3	30000	22680000	0.13	0.38	0.13%	0.02%
Totals		163						
(ISC/ESU/NESU etc)								
GROUPS								
Astoria		5	30000	37800000	0.21	0.63	0.22%	0.04%
Baltimore		6	30000	45360000	0.25	0.75	0.27%	0.05%
Boston		7	30000	52920000	0.29	0.88	0.31%	0.06%
Buffalo		6	30000	45360000	0.25	0.75	0.27%	0.05%
Cape Hatteras		5	30000	37800000	0.21	0.63	0.22%	0.04%
Cape May		7	30000	52920000	0.29	0.88	0.31%	0.06%
Charleston		4	30000	30240000	0.17	0.50	0.18%	0.03%
Corpus Christi		9	30000	68040000	0.38	1.13	0.40%	0.07%
Detroit		8	30000	60480000	0.33	1.00	0.35%	0.06%
Eastern Shore		5	30000	37800000	0.21	0.63	0.22%	0.04%
Fort Macon		3	30000	22680000	0.13	0.38	0.13%	0.02%
Galveston		8	30000	60480000	0.33	1.00	0.35%	0.06%
Grand Haven		5	30000	37800000	0.21	0.63	0.22%	0.04%
Hampton Roads		5	30000	37800000	0.21	0.63	0.22%	0.04%

Table 3-4: Communications Circuit Estimates (Cont.)

FLS								
UNIT DESCRIPTION	**Count**	**Peak concurrent users**	**Total Bytes (per user per day)**	**Total Bytes (annual)**	**Peak load Kbits/sec**	**Peak load plus 'Future Growth Factor'**	**Total FLS activity to site**	**Percent T1 pipe t site**
Humboldt Bay		4	30000	30240000	0.17	0.50	0.18%	0.03
Ketchikan		1	30000	7560000	0.04	0.13	0.04%	0.01
Key West		9	30000	68040000	0.38	1.13	0.40%	0.07
Long Island		7	30000	52920000	0.29	0.88	0.31%	0.06
Los Angeles		3	30000	22680000	0.13	0.38	0.13%	0.02
Mayport		5	30000	37800000	0.21	0.63	0.22%	0.04
Miami		3	30000	22680000	0.13	0.38	0.13%	0.02
Milwaukee		7	30000	52920000	0.29	0.88	0.31%	0.06
Mississippi, Lower		11	30000	83160000	0.46	1.38	0.49%	0.09
Mississippi, Upper		9	30000	68040000	0.38	1.13	0.40%	0.07
Mobile		11	30000	83160000	0.46	1.38	0.49%	0.09
Montery		5	30000	37800000	0.21	0.63	0.22%	0.04
Moriches		8	30000	60480000	0.33	1.00	0.35%	0.06
New Orleans		3	30000	22680000	0.13	0.38	0.13%	0.02
New York		8	30000	60480000	0.33	1.00	0.35%	0.06
North Bend		6	30000	45360000	0.25	0.75	0.27%	0.05
Ohio Valley		8	30000	60480000	0.33	1.00	0.35%	0.06
Philadelphia		4	30000	30240000	0.17	0.50	0.18%	0.03
Port Angeles		6	30000	45360000	0.25	0.75	0.27%	0.05
Portland, ME		7	30000	52920000	0.29	0.88	0.31%	0.06
Portland, OR		5	30000	37800000	0.21	0.63	0.22%	0.04
San Diego		1	30000	7560000	0.04	0.13	0.04%	0.01
San Francisco		8	30000	60480000	0.33	1.00	0.35%	0.06
Sandy Hook		6	30000	45360000	0.25	0.75	0.27%	0.05
Sault Ste. Marie		8	30000	60480000	0.33	1.00	0.35%	0.06
Seattle		4	30000	30240000	0.17	0.50	0.18%	0.03
Southwest Harbor		10	30000	75600000	0.42	1.25	0.44%	0.08
St. Petersberg		7	30000	52920000	0.29	0.88	0.31%	0.06
Woods Hole		10	30000	75600000	0.42	1.25	0.44%	0.08
Group sub total		**267**						
Major sub total		**645**						
ISC/ESU/NESU sub-total		**163**						
GRAND TOTAL						**282.90**	**Kbits/sec**	
			Percent of one T-1			**18.32%**		
		Count	= Taken from FLS study					
		Peak concurrent users	= Taken from FLS study					
		Total Bytes (per user per day)	= Taken from FLS study					
		Total Bytes (annual)	= Peak concurrent users* Total Bytes/user per day* Work year in days (252)					
		Peak load Kbits/sec	= Total Bytes (annual)/ FLS seconds/work year (1814400)* 10 (bits/byte)/ 1000					
		Peak load plus 'Future Growth Factor'	= Peak load Kbits/sec* Future Growth Factor (3)					
		Total FLS activity to site	= Peak load Kbits per sec/ Total peak load Kbits/sec					
		Percent of T1 pipe to site	= Peak load plus 'Future Growth Factor'/ 1544 Kbits per second (T1 speed)					

Table 3-5: Peak Bandwidth by Mission

OSC Martinsburg Circuits			
Mission	**Peak Load Users**	**Peak Load KBits/sec**	**Comments**
WWM/ATON *		*50*	Automated NOTAM U/W & inport
ATONIS *		*100*	
SAR *		*50*	CASP for OPCENs
SARMIS *		*50*	
IO/MSA			U/W NOTAMs
CVS			
MEP			
PSS			
MSN *		*300*	
ELT/MLE			Tactical upload & download
LEIS *		*200*	
CP/DO			Tactical upload & download
RBS			
Intel			
Logistics (Fleet)			
FLS	1076	282.90	
Logistics (Aviation)			
ALMIS			AR&SC Elizabeth City is host site
Personnel & Training		384	Video training
PMIS II	1976	189.88	
Health & Safety		*50*	Medical record imagery
Finance & Contracts			
LUFS/STAR *		*200*	Electronic commerce incl eng diagram transmission
Legal			Case File transfers
E-mail *		*200*	
Record Message System *		*200*	
GRAND TOTAL	*	**2256.78**	
Percent of T-1		**146%**	
*** Estimate not backed by definitive study**			

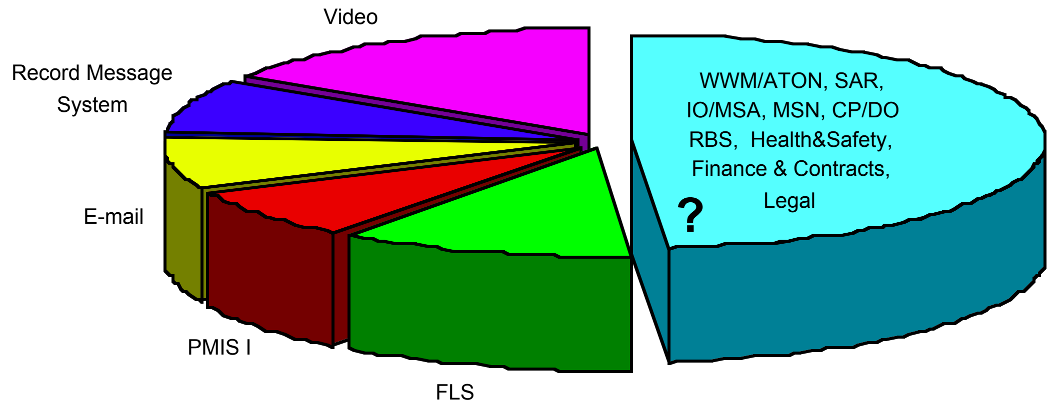


Figure 3-4: OSC Martinsburg Peak Bandwidth Estimates

Note: This diagram represents an estimate of the peak bandwidth that communications circuits at OSC Martinsburg would be required to support. The total estimate is approximately 2200 kbps (see Table 3-5). This is equivalent to about one and one-half T1 circuits. Currently OSC Martinsburg has circuits homed to its site totaling more than five

T1s. Those circuits are not fully utilized now, but some further analysis is required to refine the future requirements which are expected to be much higher than current needs.

It must be emphasized that only FLS and PMIS application managers have quantified their requirements. More work must be accomplished to properly quantify the bandwidth needs of E-mail, the Record Message System, and the programs labeled in the blue pie slice above.

When more definitive data is available, bandwidth requirements throughout the entire WAN can be projected and represented by similar tables and diagrams.

This data will be critical to effectively sizing the network. Most importantly, it will enable proactive network management to cost effectively meet all requirements and missions.

4. TECHNOLOGY ASSESSMENT

4.1 Introduction

Up to this point, we have accomplished two very important tasks. First, by completing a thorough review of all pertinent government furnished information (GFI), and visits to several Coast Guard shore and mobile commands, we have documented the Coast Guard's telecommunication system baseline (as-is) architecture (described in Chapter 2). This effort was followed by a set of detailed interviews with key Headquarters Program Managers and Staff, which complemented the research and analysis that was accomplished in Chapter 2. From this, we developed a comprehensive list of future telecommunications requirements which are provided in Chapter 3.

In this chapter, we will assess several technology areas: (1) Data Networking, (2) Mobile Communications, and (3) Requirements for Interoperability with DoD. We will analyze networking technologies at a high level just to determine their potential for addressing current and future requirements, and their impacts on the Coast Guard's future architecture. We will assess the relevant technologies and develop a list of alternative solutions, and future architectures, capable of satisfying Program Manager requirements. For each technology, we will answer three very important questions: What is it? What will it do for the Coast Guard? And, What is a rough estimate of its cost? The list of alternatives will be analyzed more completely in the next Chapter of the TCP.

Within the telecommunications system, there exists several dedicated networks to serve the Aviation, Communication Station, and Radionavigation communities. The choice of standards and architecture for the Coast Guard network will consider these networks. A good choice of Coast Guard network systems will allow these dedicated networks to seemlessly migrate onto the standard Coast Guard network. This should result in lower operating, training, and maintenance costs, while meeting these systems standards for survivability and reliability.

4.2 Data Networking Alternatives

In this section, we will discuss several alternatives for meeting the Coast Guard's current and future data networking requirements. These alternatives, which encompass both dedicated and on-demand networking connections, include X.25, Asynchronous Transfer Mode (ATM), Frame Relay, Integrated Services Digital Network (ISDN), Point-to-Point networking services, and Very Small Aperture Terminal (VSAT) networking. It is important to keep in mind, while planning the future network architecture, that the Defense Message System (DMS) is a requirement that will have a considerable impact on the Coast Guard's data networking solution. DMS implementation is scheduled to begin in 1997 as the backbone infrastructure is developed and activities involved in initial test and evaluation of DMS contract products begin to cut over. The expected service-wide cutover date is 1999. DMS will be discussed in greater detail later on in this section.

For each alternative, overall operating costs (where available) include circuit installation charges and basic monthly rates, along with equipment purchase costs. Costs were determined using a sample network configuration consisting of two remote units (Atlantic and Pacific Area) connected to a central site (OSC Martinsburg). This limited network architecture is considered adequate for high-level cost comparison purposes. More detailed life-cycle costong of selected alternatives will be accomplished in Chapter 5.

(Note: It is understood that telecommunication costs and system availability in Alaska and Hawaii may differ from CONUS networking solutions.

Wherever it is cost effective and possible, the network will be designed to minimize single point failures, critical nodes, and to ensure the highest reliability and survivability practical. This is especially important due to the nature of Coast Guard missions—the demand for services is greatest in times of disaster, such as earthquakes, hurricanes, and floods. It is at these very times that the widespread unavailability of traditional communications is most likely. This should allow us to effectively weigh, later on in the TCP, the potentials and costs of matrixed systems, back-up options, and fully diverse systems. The costing issues of selected alternatives will be discussed in greater detail in Chapter 5.

4.2.1 Packet-Switched Data Network

The current Coast Guard Data Network (CGDN) is an X.25 packet-switched data communications network connecting all large and most small Coast Guard units. The CGDN provides the primary transmission media for day-to-day, unclassified individual (electronic mail) and organizational record communications. It consists of both leased circuits and Coast Guard owned and leased switching facilities.

Data transaction communications is accomplished by either imbedding the transaction in the mail message or attaching a file of transactions to the message. Using the X.25 protocol, a single message is broken into packets which are transmitted when circuit time is available and re-assembled at the receiving end to reconstitute the message. The X.25 software protocol assigns identifiers to each message packet to enable correct reassembly at the receiving end. Error correction is built into the X.25 protocol, since packet-switched networks are relatively noisy. This adds to the overhead for each packet transmitted over the network. X.25 was designed in an era of data communications speeds of 300 to 1200 bps. Older switches, built for this protocol, have a capacity to handle bandwidths of up to 56 kbps. To obtain higher bandwidths, older switches need to be replaced with newer ones.

The CGDN consists of 56 kbps circuits connecting major nodes (Figure 4-1) located at Coast Guard Headquarters, Area and District Offices, and the Operations Systems Center (OSC). This portion of the network is called the backbone. Each major node (except Districts 14 and 17) is connected to at least two other nodes by these high speed circuits to ensure alternate routing in case of a single circuit failure.

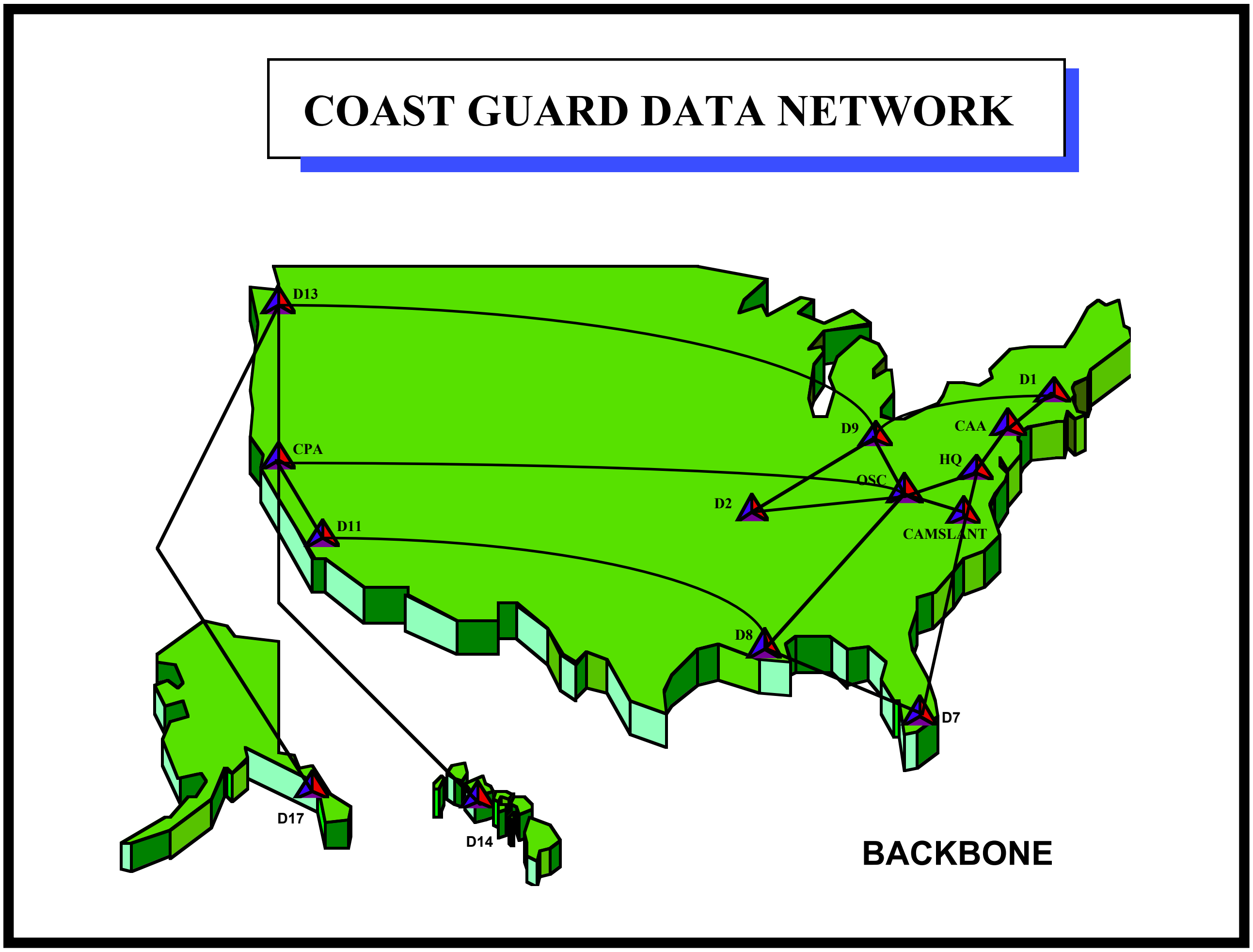


Figure 4-1: CGDN Backbone Network

Secondary nodes are installed at Groups, Marine Safety Offices (MSOs), Air Stations, Communication Stations (COMMSTAs), and other selected units. The nodes at these sites are connected to the backbone through one of the major nodes, typically the district to which they are assigned. Transmissions between secondary and primary nodes may be either 56 or 9.6 kbps, depending on traffic volume.

Although most CGDN locations are provided access via dedicated circuits, traffic volume at some units does not justify this cost. At these units, access to the CGDN is made available via a dial-up telephone line through the local commercial carrier. This type of connectivity is frequently referred to as "virtual" access. The singular disadvantage of virtual access is that traffic for all users, at these locations, must be held in the system until the users dial into the network. Transmission speed, for this type of connectivity, is 2400 bps.

A network management system is used to monitor the system and locate problems. As implemented, the CGDN normally operates unattended. Support for CGDN equipment is expected to be available until the year 2000.

4.2.2 Asynchronous Transfer Mode (ATM)

ATM is one of several new and emerging networking technologies that addresses today’s networking problems. The need for a world-wide, international standard to allow interoperability of information, regardless of the type of information or system, has been the catalyst for ATM development.

Historically, there have been separate methods used for the transmission of information among users on Local Area Networks (LANs), versus users on Wide Area Networks (WANs). This situation has added to the complexity of networking, as user's needs for connectivity expand from the LAN to metropolitan, national, and finally world-wide connectivity. ATM is a method of communication which can be used as the basis for both LAN and WAN technologies. Over time, as ATM continues to be deployed, one standard, seamless ATM network will be formed. Caution should be used, however, in planning an ATM networking solution, since ATM technology is new and not yet standardized across the vendors for WAN implementations. The vendors are working toward those standards and may have them in place before the Coast Guard finalizes its network modernization.

Currently, separate networks are used, in most cases, to carry voice, data and video information. Why? Because each of these traffic types have different characteristics. This, however, is not the case with ATM. Separate networks will not be required. ATM is currently the only standards-based technology which can accommodate the simultaneous transmission of data, voice and video.

ATM networks can be complicated and will likely require significant technician training for Coast Guard implementation. As described above, ATM is a state-of-the-art, emerging standard for communications which will soon be available at speeds up to 622 Mbps, using a layered architecture. This allows multiple services, like voice, data, and video, to be mixed over a single network.

ATM has several key benefits:

- ATM can provide a single network for voice, data, video services;
- Due to its high speed and the integration of traffic types, ATM will enable the creation and expansion of new applications, such as multimedia to the desktop;
- ATM can be transported over twisted pair, coax, and fiber optic cable;
- Embedded networks will be able to gain the benefits of ATM incrementally, upgrading portions of the network based on new application requirements and business needs;
- ATM is evolving into a standard technology for local, campus/backbone, and public and private wide area services. This uniformity is intended to simplify network management by using the same technology for all levels of the network;
- ATM is scaleable and flexible; and

- ATM coexists with current LAN/WAN technology, and will integrate with numerous existing network technologies at several levels (i.e., Frame Relay, Ethernet, TCP/IP, etc.).

Figure 4-2 shows an example of an integrated voice, data, and video network connecting three remote sites using an ATM technology solution.

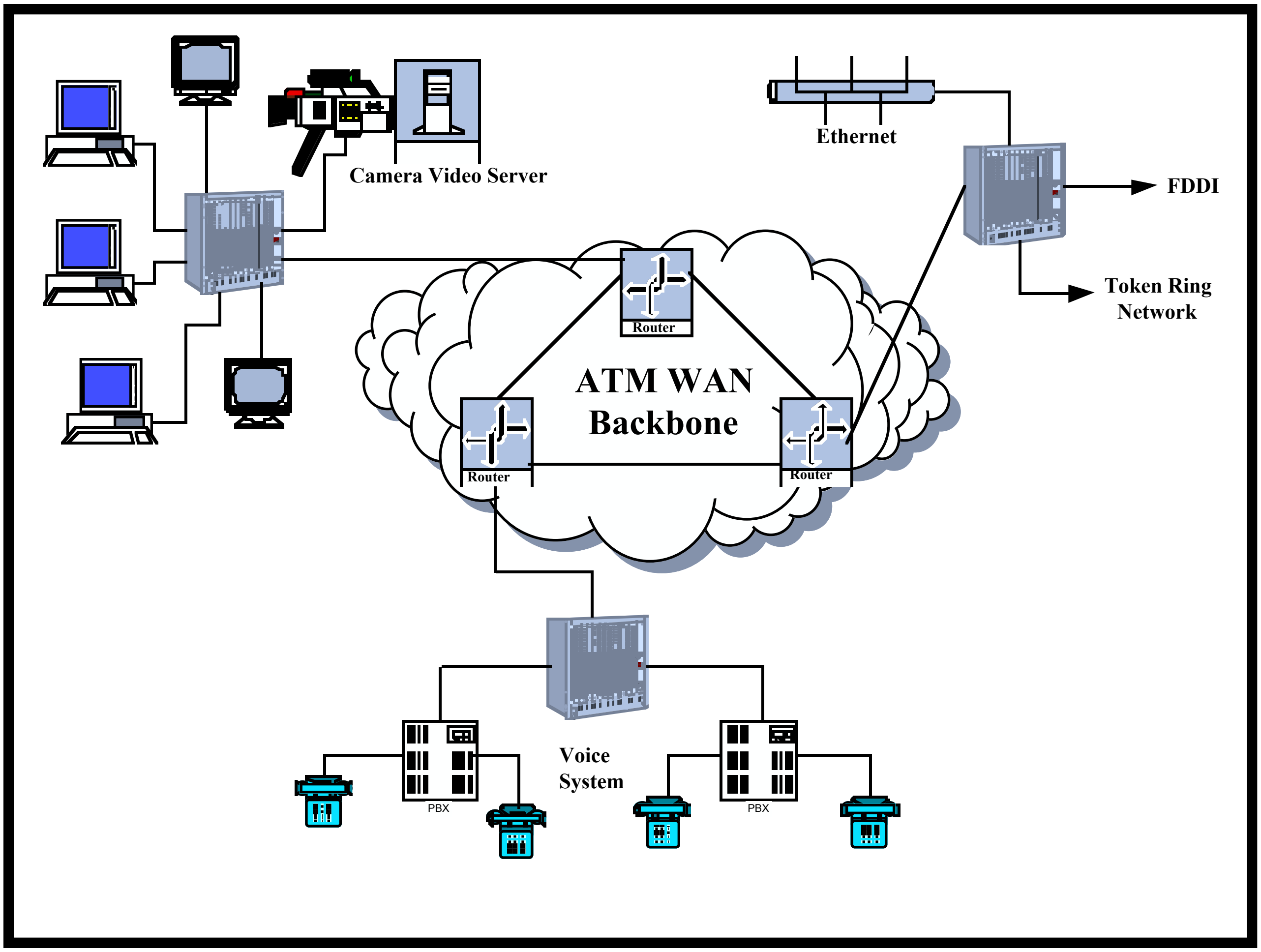


Figure 4-2: Typical ATM Network

Table 4-1, below, identifies the configuration of equipment and services needed to provide ATM communications from the Ethernet LAN at two remote sites (Atlantic and Pacific Area Offices) to a central site (OSC Martinsburg).

Table 4-1: Asynchronous Transfer Mode (ATM)

Item	OSC Martinsburg	Pacific Area	Atlantic Area	Total
Access Speed	T3	T3	T3	
Port Speed	T3	T3	T3	
CIR Speed	2 Mbps	2 Mbps	2 Mbps	
Initial Costs:				
Access/install.	$3,810	$6,620	$3,810	$14,240
Port/install.	$1,500	$1,500	$1,500	$4,500
PVC/install.		$75	$75	$150
Routers - Cisco 4500	$8,100	$8,100	$8,100	$24,300
Sub-total:				**$43,190**
Recurring Costs:				
Port/monthly	$6,000	$6,000	$6,000	$18,000
Access/monthly	$16,000	$7,870	$11,070	$34,940
PVC/monthly		$1,100	$1,100	$2,200
Sub-total:			**Monthly:**	**$55,140**

Point of Contact: Maryland West, AT&T FTS 2000, (202) 776-6481

4.2.3 Frame Relay

Frame Relay is a wide area data communications service designed specifically for bandwidth-intensive and delay-sensitive data applications. It can provide access speeds up to 45 Mbps (T3) while using the principle of shared bandwidth to provide for virtual connections between locations. Frame Relay is a relatively new technology which works over digital and analog lines. This makes Frame Relay very durable. It may be replaced with ATM services in the distant future. However, ATM is fully compatible with Frame Relay and users would not have to change equipment to access the faster ATM circuits.

Figure 4-3, below, shows a typical Frame Relay Network with three remote sites.

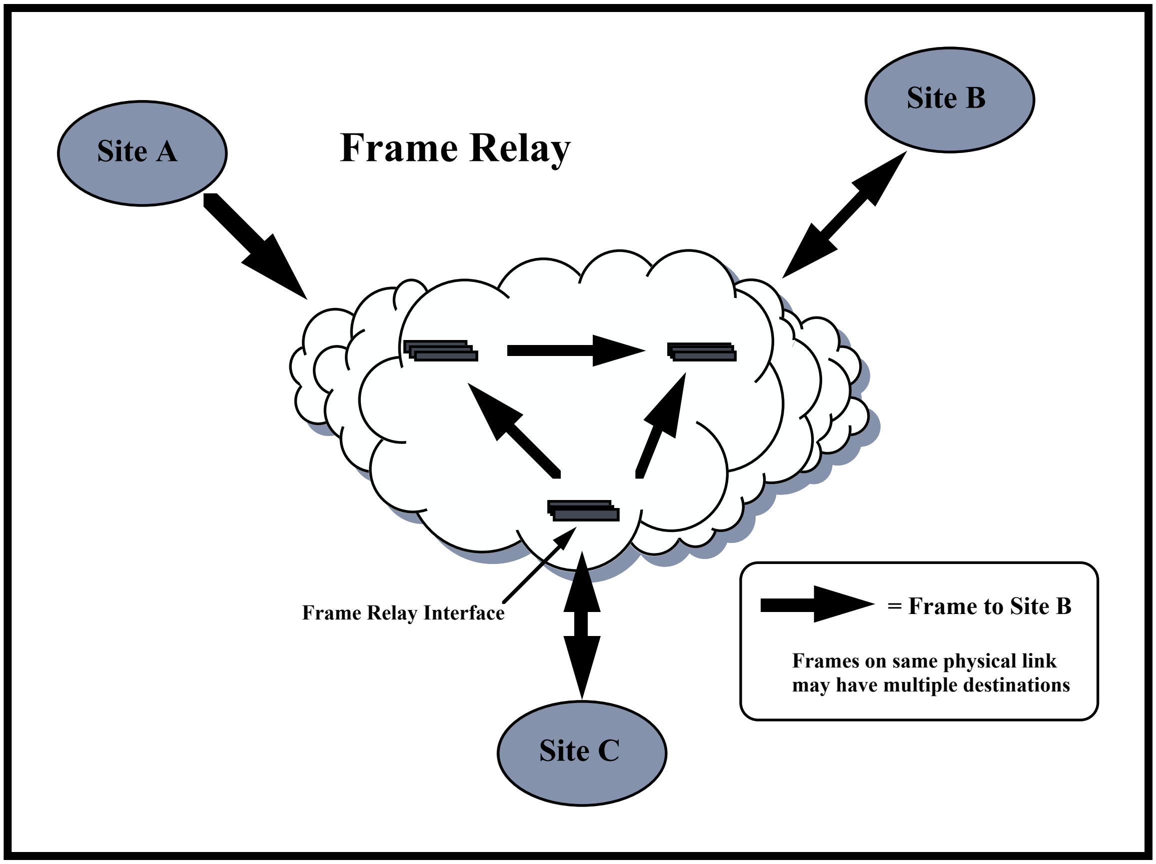


Figure 4-3: Frame Relay Network

Since Frame Relay is a new and growing technology, there should be no concern about this technology becoming obsolete in the near future. Frame Relay services are available nation-wide, making this technology a good choice for all high volume communications. It is very reliable and will meet the Coast Guard's current and future response time and traffic volume requirements.

The virtually noise free and quick connection times of Frame Relay lines cannot be matched. Frame Relay compares well with ISDN services for reliability and far outmatches normal voice grade telephone communications.

For meeting network maintainability and expandability requirements, the long distance carrier, on the FTS2000 contract, maintains the Frame Relay network and users pay for time on the network. Therefore, a call to the long distance provider should be all that is needed to fix Frame Relay line problems.

The Committed Information Rate (CIR) and Peak Bandwidth are both flexible and expandable from a low bandwidth of 32 kbps to bandwidths as high as 1.544 Mbps. The CIR and Peak Bandwidth will be chosen when buying the Frame Relay service. At a future date, when users need a higher CIR or Peak Bandwidth, they can replace the lower bandwidth with a high bandwidth for either CIR or Peak. Frame Relay offers better performance and expandability than ISDN or regular dedicated circuits.

In addition to data, Frame Relay can also handle voice conversations, fax transmissions, and teleconferencing. It also has a flexible bandwidth for bursty data transmissions. Therefore, users could use a higher bandwidth for bursty data and a lower bandwidth for normal low-volume usage, and only pay for the higher bandwidth when they need it.

The FTS2000 contract offers a Frame Relay network management feature that can be used to monitor the entire network from a central site and also account for traffic by user. This system would quickly alert network managers to any problems with the network.

A Frame Relay virtual circuit is similar to a typical telephone cable which may contain multiple pairs of wires, one for each individual conversation. In Frame Relay, a single physical interface may contain several individual conversations. However, unlike a typical telephone call, multiple logical channels exist in a single physical circuit. Also, unlike a typical telephone call, no network resources are used when there is "silence" on the line. This is the real power of Frame Relay.

Frame Relay scales itself based on user need. Some of the major INTERNET service providers are deploying high-speed Frame Relay backbones to guarantee customers' network availability. Because of increasing demands for more bandwidth, service providers are choosing Frame Relay to provide high performance, cost-effective solutions to their customers.

High-speed Frame Relay provides a viable alternative to end users who are not ready to commit to ATM services. With the ability to reach T3 speeds (equal to 28 T1s or 44.736 Mbps), the investment in Frame Relay equipment and services can be maximized for years to come.

Frame Relay represents the alternative requiring the least amount of training for Coast Guard personnel. Since it is an evolution of the X.25 protocol, the Coast Guard technicians should be familiar with most of the language and procedures surrounding Frame Relay.

Table 4-2, on the next page, identifies the configuration of equipment and services needed to provide Frame Relay communications from the Ethernet LAN at two remote sites (Atlantic and Pacific Area Offices) to a central site (OSC Martinsburg).

Table 4-2: Frame Relay Configuration

Item	OSC Martinsburg	Pacific Area	Atlantic Area	Total
Access Speed	T1	T1	T1	
Port Speed	1536	1536	1536	
CIR Speed		512 kbps	512 kbps	
Initial Costs:				
Access/install.	$1,555	$1,555	$1,555	$4,665
PVC/install.		$39	$39	$78
Port/install.	$467	$467	$467	$1,401
Routers - Cisco 4500	$8,100	$8,100	$8,100	$24,300
Sub-total:				**$30,444**
Recurring Costs:				
Access/monthly	$362	$362	$362	$1,086
Port/monthly	$1,831	$1,831	$1,831	$5,493
PVC/monthly		$947	$947	$1,894
Sub-total:			**Monthly:**	**$8,473**

Point of Contact: Maryland West, AT&T FTS 2000, (202) 776-6481

4.2.4 Integrated Services Digital Network (ISDN)

ISDN (also known as Digital Subscriber Line (DSL)) is a totally new concept of what the world's telephone system should be. ISDN's vision is to overcome the deficiencies in today's public switched phone network by providing an international telecommunications standard for transmitting voice, data, and video over digital lines at 64 kbps. They expect to accomplish this by making all transmission circuits end-to-end digital, by adopting a standard out-of-band signaling system, and by bringing significantly more bandwidth to the desktop.

ISDN uses circuit-switched bearer channels (B channels) to carry voice and data, and uses a separate data channel (D channel) for control signals via a packet-switched network. This out-of-band D channel allows for features such as call forwarding and call waiting.

One of the best features of ISDN is the speed of dialing. Instead of 20 seconds for a call to go through on today's analog network, it takes less than a second with ISDN.

The following are examples of available ISDN services:

- Call waiting: If a line is busy and another call comes in, the user knows who is calling. He can then accept, reject, ignore, or transfer the call;
- Citywide Centrex: This provides a number of services, including specialized numbering and dialing plans, and central management of all ISDN terminals, including PBXs, key systems, etc.;

- Credit card calling: Automatic billing of calls into accounts independent of the calling line(s);
- Caller Identification: Provides calling party identification to the called party. Such information may flash across the screen of an ISDN phone or be announced by a synthesized voice. The called party can then accept, reject, or transfer the call. If the called party is not there, then his/her phone will automatically record the incoming call's phone number and allow automatic callbacks when he/she returns or calls in from elsewhere;
- Desktop Videoconferencing: Provides full motion video display of the person you are talking with;
- E-mail: ISDN can carry information to and from unattended phones as long as they are equipped with proper hardware and software;
- INTERNET Access: Provides you with the capability to browse the INTERNET at 128 kbps rather than at 28.8 kbps, which is the fastest speed available with analog modems today.
- Simultaneous Data Calls: Two users can talk and exchange information at the same time.

There are also several new customer services which will significantly broaden the number of useful new services the ISDN telephone network of tomorrow will be able to deliver. One example is the Consultative Committee on International Telegraphy and Telephony (CCITT) Signaling System 7, which removes all phone signaling from the present network onto a separate packet switched data network. This provides enormous economies of bandwidth, and also broadens the information that is generated by a call, or call attempt.

ISDN comes today in two basic flavors:

- Basic Rate Interface (BRI), which provides two 64 kbps B channels and one 16 kbps D channel (2B+D) for a total of 144 kbps. BRI lines, usually designed for the desktop, are provided by the local telephone company, usually for a flat monthly fee. ISDN BRI can give you full motion videoconferencing and ultrafast data communications; and

- Primary Rate Interface (PRI), which provides 23 B channels and one 64 kbps D channel (23B+D), equivalent to a T1. PRI services are designed for telephone switches, computer telephony, and voice processing systems. They are provided by long distance carriers, such as AT&T, over existing phone lines, and are available on the FTS2000 contract.

With ISDN, communications support to large and small Coast Guard units would be provided using ISDN BRI lines, wherever they are available, and by using voice grade FTS2000 dial-up lines from locations where ISDN BRI service is not available. Over a period of time, the dial-up sites could be replaced by BRI services, as ISDN BRI services become available at new locations. Figure 4-4 is an example of an ISDN BRI architecture.

Dial-up services will use the Plain Old Telephone Service (POTS), which is the basic service supplying standard single-line telephones, telephone lines, and access to the public switched network. This would be provided under the FTS2000 contract.

Note: The cost of analog point-to-point services is beginning to climb. Costs are expected to continue to rise as vendors and customers migrate to new standards and digital technology.

The potential complexity of ISDN can result in an equally intensive training problem as discussed in the ATM section.

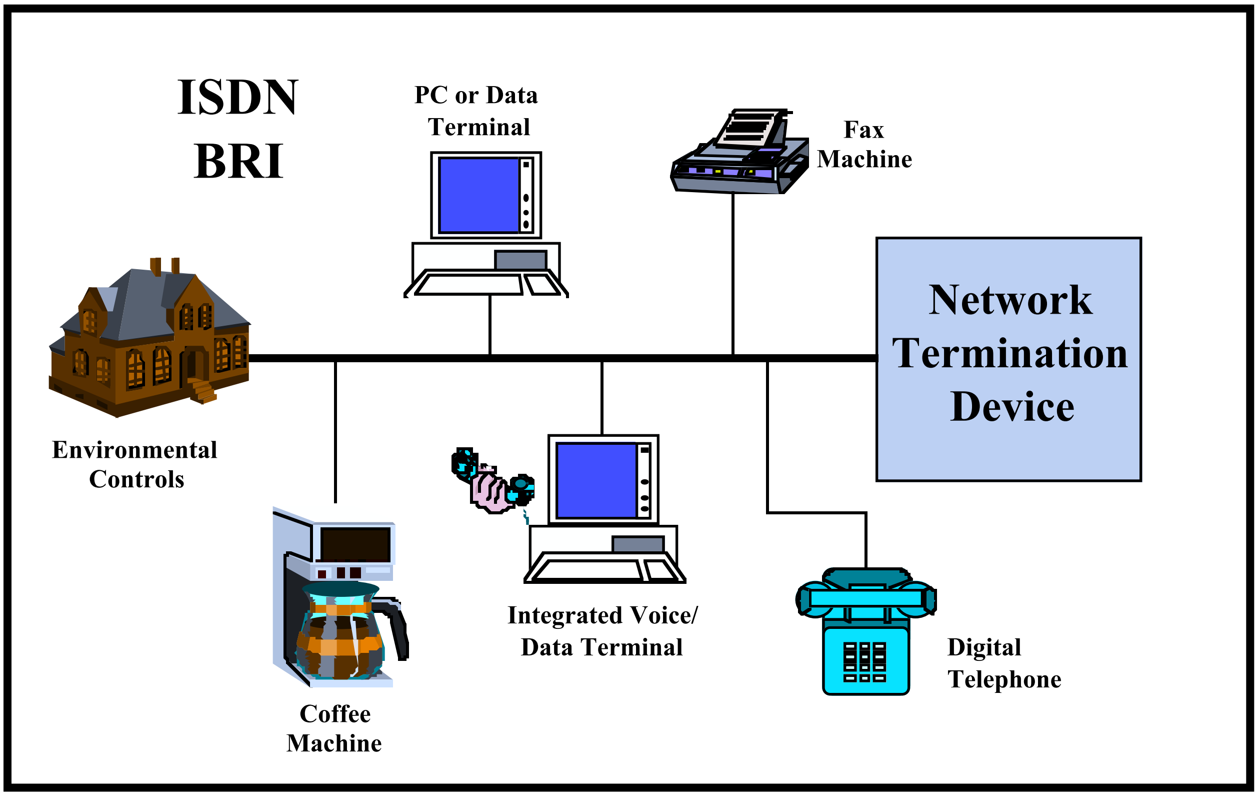


Figure 4-4: ISDN BRI Architecture

Table 4-3, below, identifies the configuration of equipment and services needed to provide ISDN full-time (i.e., 24 hrs./day) communications from the Ethernet LAN at two remote sites (Atlantic and Pacific Area Offices) to a central site (OSC Martinsburg). The requirement may not be a 24 hour virtual circuit, but it is the only way to guarantee a connection like the other WANs provide.

Table 4-3: ISDN Configuration

Item	OSC Martinsburg	Pacific Area	Atlantic Area	Total
Access Speed	T1	T1	T1	
Initial Costs:				
Access/install.	$1,555	$1,555	$1,555	$4,665
Routers - Cisco 4500	$8,100	$8,100	$8,100	$24,300
Sub-total:				**$28,965**
Recurring Costs:				
Access/monthly	$373	$373	$373	$1,119
Monthly Usage		$112,608	$112,608	$225,216
Sub-total:			**Monthly:**	**$226,335**

Point of Contact: Maryland West, AT&T FTS 2000, (202) 776-6481

4.2.5 Point-to-Point Service:

This is the most widely implemented form of wide-area networking. It is available anywhere in the world and is the industry standard. Therefore, all router vendors supply the capability by default. In some cases, it may be more expensive than some other forms of WAN implementation, but it works very well in small scale installations. In large scale installations, it can be difficult to configure and maintain all of the necessary interfaces to effectively and efficiently manage the WAN. This may require significant training for Coast Guard technicians to overcome these configuration problems.

Many units have a need for high-speed transfer of data between large locations. The transfer process may be needed for long time periods each day, as in the case of near-continuous operations involved in financial or scientific applications.

Dedicated T1 service meets this need by providing high-speed digital data transmission at 1.544 Mbps. The service is available 24 hours a day and is priced on a fixed monthly basis. Therefore, it may be more economical to the heavy user who needs the service for long-time periods.

The primary benefits of using dedicated T1 service for this application include:

- The service delivers high-quality performance on an end-to-end basis and is designed for data applications by using digital facilities. The high-speed (1.544 Mbps) allows increased throughput of the data, which saves time and increases productivity.
- The service is cost effective for high-volume users who require availability for long periods of time each month. The rates are not usage-based; therefore, the user has availability 24 hours a day for a fixed monthly rate.
- The service has high reliability.

Dedicated T1 service provides point-to-point (only) transmission at a rate of 1.5 Mbps. This would be enough capacity to transmit the contents of an entire high-density floppy disk in less than 8 seconds. Dedicated T1 is often used to transmit Computer Aided Design (CAD) drawings between locations, to connect LANs, and to tie mainframe computers together, allowing them to share processing power. Figure 4-5 shows a typical point-to-point connection between two remote locations and a central site.

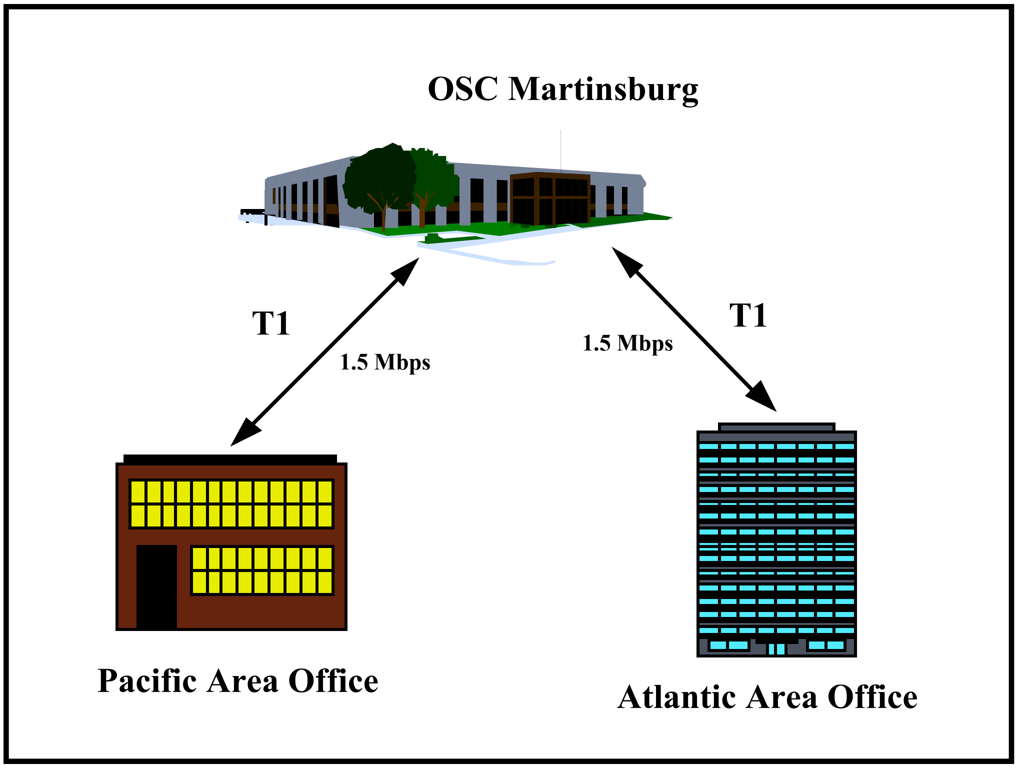


Figure 4-5: Point-to-Point Connection

A user with dedicated 56 kbps service might find that the application requires slightly faster data throughput, but not enough to justify the purchase of a dedicated T1 facility. The solution may be to order fractional T1 service, which affords easy and economical migration to higher data transmission speeds. In many cases, users can double their transmission rates without doubling the circuit price.

Fractional T1 service offers the following benefits for this application:

- The service provides high quality, end-to-end, digital transmission;
- Customer can choose between 11 transmission speeds, providing the right price and performance for the agency's application; and
- Fractional T1 provides data rates ranging from 128 to 768 kbps, in increments of 64 kbps.

Table 4-4 below, identifies the configuration of equipment and services needed to provide point-to-point communications from the Ethernet LAN at two remote sites (Atlantic and Pacific Area Offices) to a central site (OSC Martinsburg).

Table 4-4: Point-to-Point Ethernet (T1 speed)

Item	OSC Martinsburg	Pacific Area	Atlantic Area	Total
Access Speed	T1	T1	T1	
Initial Costs:				
Access/install.		$3,110	$3,110	$6,220
Routers - Cisco 4500	$8,100	$8,100	$8,100	$24,300
Sub-total:				**$30,520**
Recurring Costs:				
Access/monthly		$6,818	$1,734	$8,552
Sub-total:			**Monthly:**	**$8,552**

Point of Contact: Maryland West, AT&T FTS 2000, (202) 776-6481

4.2.6 Very Small Aperture Terminal (VSAT) Networking:

New technology is being developed that will offer high speed access to the INTERNET via a digital satellite system. This technology will provide data services that are several times faster than ISDN and far less expensive. Large files can be transferred at 3 Mbps, with full broadcast channel capacity of 12 Mbps. This system also offers Digital Encryption Standard (DES) compatibility.

Low cost commercial two-way VSAT networking is well into the developmental stage, and maritime mobile VSAT technology has been demonstrated as well. For these reasons, a VSAT network may soon be practically expandable to most Coast Guard units—shore, mobile, and deployable. Also, with planned entrances into this market by RCA, Microsoft, Sony, and Primestar, intense competition should rapidly reduce costs and improve features. This, and a lack of single point failure commonality with the terrestrial networks, should provide major advantages of reliability and survivability either as a back-up or primary system.

Maritime Mobile VSAT technology is now available using commercial off-the-shelf hardware for one-way receipt of data and two-way satellite telephone. Vendors plan to introduce two-way fixed land as well as two-way marine and mobile VSAT data units in 1997. These services provide coverage in the continental U.S. and waters to approximately 200 miles offshore.

Hughes Network Systems now offers a VSAT networking service called DirecPC, which currently provides high speed, one-way, receive-only access to the INTERNET (Figure 4-6).

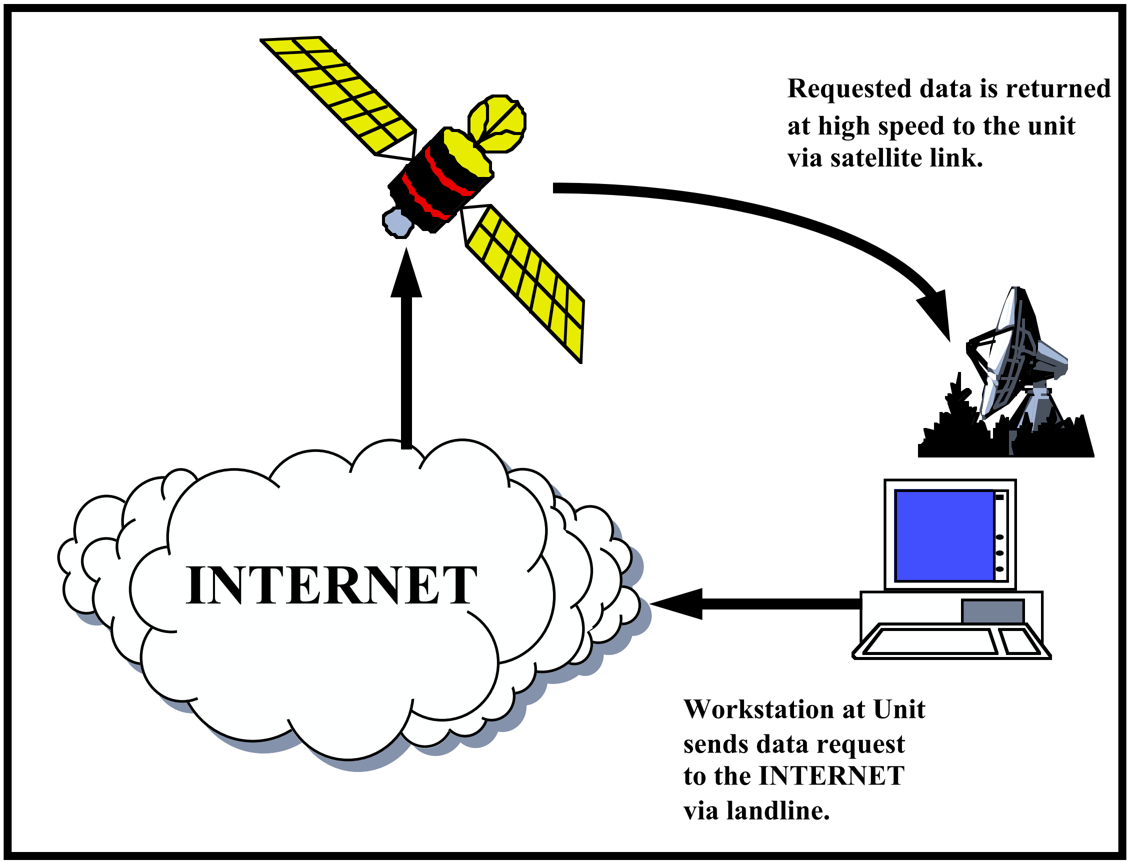


Figure 4-6: DirecPC High Speed INTERNET Service

With Hughes Corporation's DirecPC Digital Package Delivery service, users can have access to one-way broadcast of digital information to an unlimited number of locations. This information includes electronic files, software, documents, and computer-based training. Users can select either a pre-scheduled broadcast or on-demand service.

To transmit information via the DirecPC broadcast, the user sends the broadcast information, along with its corresponding address and schedule, to the service provider's Network Operations Center. From there, it is broadcast via Ku-band satellite to the designated addressees (Figure 4-7).

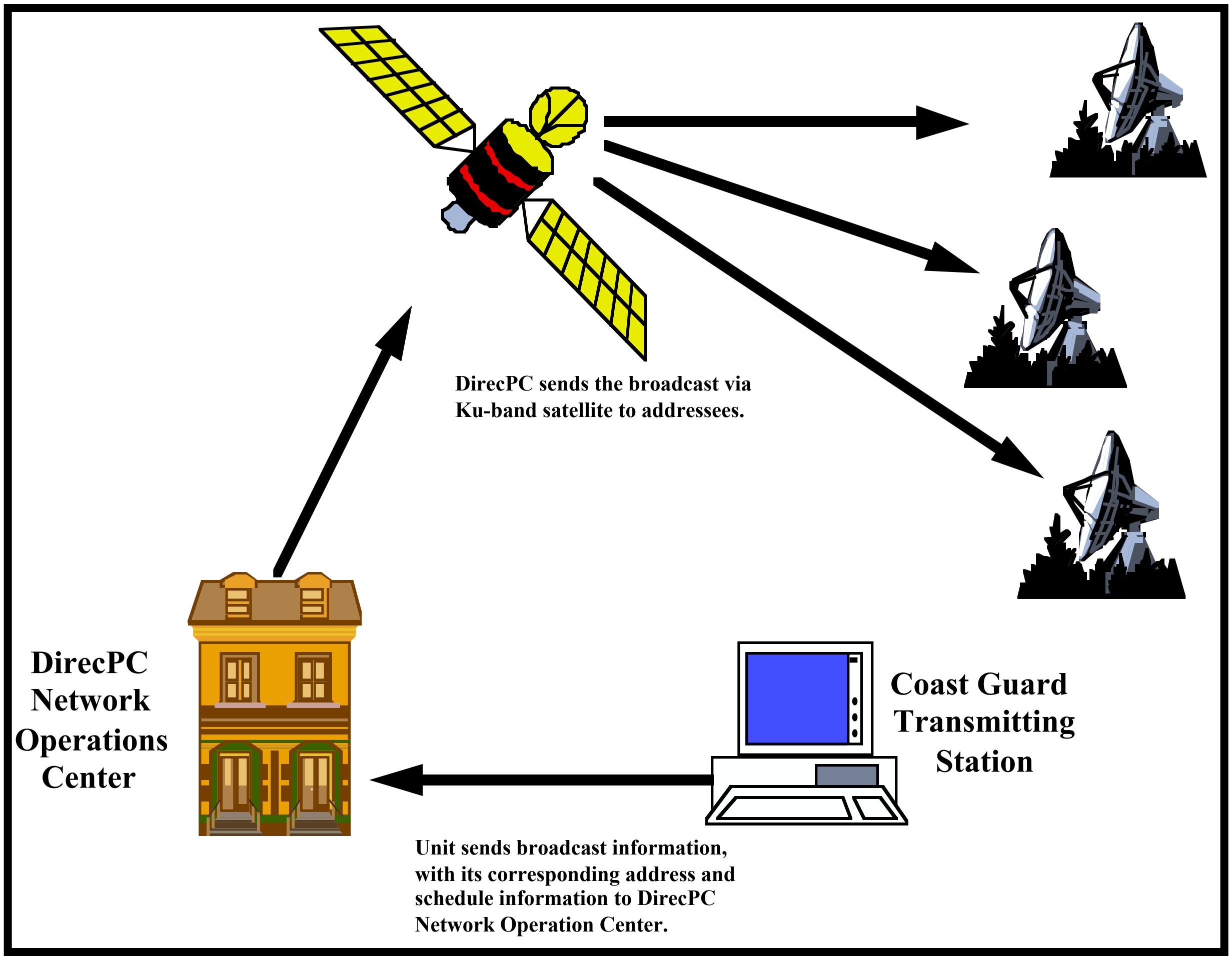


Figure 4-7: DirecPC Broadcast Service

DirecPC provides users desktop video and audio service, and also the capability of transmitting information at high speeds to an unlimited number of sites at a relatively low cost. The service is expandable and the 12Mbps digital channel allows for increased broadcast of video and images.

DirecPC may help the Coast Guard telecommunications system run more smoothly and efficiently by providing a dedicated satellite channel with instantaneous transmission that ensures all locations receive the same information at the same time. Limited initial equipment cost allows for economy and efficient use of transmission capabilities.

In Table 4-5, below, costs are compared between ISDN, DirecPC, and Point-to-Point systems. Since any one or a combination of these systems may be used to provide full-time or back-up services, for the new network, the table shows monthly charges for full-time (24-hour) usage, and for part-time (5% of the time) backup services. ISDN costs decreased significantly, when used as a backup service, since monthly charges are base primarily on per minute usage. DirecPC remains the same because flat rate monthly service continues to be the most economical alternative under either scenario. Point-to-Point service remains the same because costs are primarily based on T1 line charges, and dedicated T1 circuits will be required for either full-time or backup systems. (Keep in mind that DirecPC is currently capable of providing INTERNET and INTRANET access services only.)

Table 4-5: DirecPC Cost Comparisons

Service:	ISDN	DirecPC	Pt-to-Pt
Description:	Low-speed digital connection	High speed digital satellite connection	Very high speed digital connection
Initial Cost:	$800	$1,349	$7,000
Monthly Charges:			
Full-time usage	$112,608	$180	$6,818
Backup system only	$5,630	$180	$6,818

POC: info@mail.direcpc.com // 1-800-DIRECPC

All you need to get started is a DirectPC Access Kit (DAK), which includes the satellite antenna, adapter card, and software. Then subscribe to your choice of services—whatever will meet your operational or administrative needs. These services include a wide range of information services and data delivery options to meet voice, data, and video requirements. DirecPC also provides the capability of protecting sensitive data during transmission by using DES encryption.

Until this technology is further developed, it may not offer the Coast Guard a viable, full-service data networking solution. However, this type of system may prove to be useful in emergencies and disasters, and also by at-sea mobile units for obtaining operational message traffic and other critical information from VSAT broadcast services. These services may provide significant cost reductions when compared with INMARSAT services, currently used where available. Since this technology is designed to be easy to install and operate, technician and operator training requirements are considered to be minimal.

4.2.7 Defense Message System

The Defense Message System (DMS) provides secure, accountable, and reliable messaging services, fully integrated with a global DoD directory service, based on Joint Staff validated requirements. It has a robust set of services that will work writer-to-reader, desktop-to desktop in DoD and externally.

With these capabilities, the Coast Guard will be able to access global directories from anywhere in the world, complete with addressing, security, and user capabilities information for all the messages sent and received from each desktop.

DMS will be implemented with commercial-off-the-shelf (COTS) products to be based on a set of international, open-system standards that provide full interoperability from writer-to-reader. Additionally, DMS will provide interfaces to and interoperability with other federal agencies, U.S. allies, the commercial sector, and the public. This is being done using a standards-based suite of products that ensure writer-to-reader messaging services and global directory capabilities, without the use of gateways.

Why is the Navy building DMS? With the Automatic Digital Network (AUTODIN), telecommunication centers were essentially using over-the-counter message technology developed in the 1960s to deal with messaging requirements presented by the 1990s.

AUTODIN does have some strong points. It is secure, reliable, and available, which is more than can usually be said for DoD’s e-mail system, of which there are 47 different flavors in use. However, AUTODIN is costly, staff intensive, incapable of passing binary files, and results in the infamous writer-to-reader message delivery delays. After all, the fastest inter-switch trunk operates at 4800 bps! In today’s environment, that is very slow.

Today’s legacy, although proprietary, e-mail capabilities offer a rich set of services for use within DoD’s local enclave. However, they lose those services when the message is transferred through one of the many DoD Simple Mail Transfer Protocol (SMTP) gateways, across the SMTP backbone, then through another gateway into another proprietary e-mail enclave. This causes problems. Those gateways aren’t secure, and they are infamous for addressing problems.

While SMTP e-mail is more flexible and easier to use than AUTODIN, it suffers from a lack of enterprise-wide management, integrity, accountability, security features, and standardization of service. In short, neither system provides optimum capabilities.

These problems, coupled with the problems of AUTODIN, are legacies of old technology. The loss of service and costs inherent in these legacies can’t be tolerated in today’s environment.

As a solution to these problems, DMS takes organizational messaging and individual e-mail messaging and brings them together in a single system based on a single set of standards. This allows different brands of standard-based products to interoperate with each other without the use of gateways.

DMS is divided into two major pieces: the infrastructure piece and end-user piece. This was done for two reasons. One was from a management perspective, ensuring DISA could manage the infrastructure, and also to be sure the local managers can maintain their piece. The infrastructure piece will be paid for by DISA, put on the ground by DISA, and managed and maintained on DoD computers. From a user perspective, the components will be provided by the services and agencies and will be managed on the desktop by the local commander. The DMS infrastructure consists of the following:

- X.400 Message Transfer Agents connecting all DMS User Agents;
- Directory System Agents (DSAs) containing distributed directory information for the entire DoD;
- Mail List Agents (MLAs) performing multiple deliveries for messages addressed to a single collective address;

- Multifunction Interpreters (MFIs) providing protocol translation for interoperability during transition, and with non-DMS systems after transition; and
- DMS Management and Control function designed to keep the infrastructure up and running.

<u>Here's the DMS solution.</u> To ensure interoperability, as well as retention of services from writer-to-reader, the elimination of gateways, by the inclusion of a common message standard for both organization and individual messages, is required. The absence of gateways will improve interoperability by providing a single addressing structure, allowing writer-to-reader security, ensuring a consistent set of services, and eliminating gateway-derived delivery difficulties. X.400 was designed with this sort of interoperability in mind.

The only protocol translations required will be those needed to communicate between DMS compliant users and users not on similar systems. These users include AUTODIN during the transition to DMS (for organizational messaging only), other (non-DMS compliant) X.400 users, and those using SMTP/MIME as the common backbone for connecting enclaves of proprietary messaging components (i.e., INTERNET users).

It is very important to understand that with secure, reliable DMS, there will be no more DD-173s, no more walking to the telecommunication centers, no more paper distribution, and paper database directories. That's over.

Figure 4-8, below, represents the DMS target architecture and depicts the DMS objective system. It is a representative sample of the DMS implemented in the year 2000 timeframe and will serve users while at home-base, traveling, or tactically deployed. Traveling users may dial-in to DMS through authenticated DISN access points. Deployed users will interface to the same messaging system as those on shore.

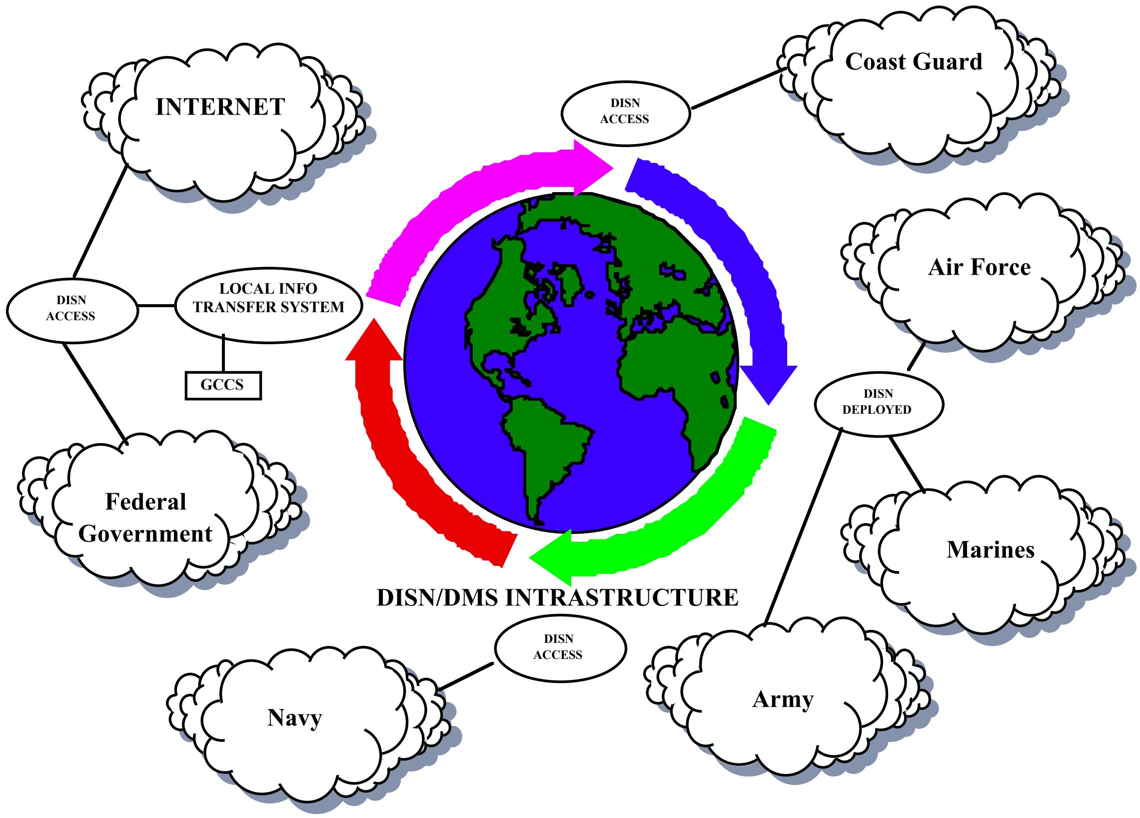


Figure 4-8: DMS Objective System

DMS Training: DMS training is being developed to provide a continuation of defense message handling and capability through the use of current trained and experienced personnel. DMS training courses will be conducted using a variety of training methods at locations world-wide. Training courses may be taught by contractor personnel or previously trained Government personnel. Training courses may be held at contractor resident training locations or conducted at DoD sites by mobile training teams. The courses may also be available through interactive courseware and video tape media.

The courses outlined below, available through DISA's contract with LORAL Federal Systems, are designed to be taught at either a Government facility or contractor site, for individual users, or by contractor personnel/Government instructors:

- Basic User Training Course (User Agent Course);
- Operating System Administrator (OSA) Course;
- Message Handling System (MHS) System Administrator Course;
- Directory System Administrator (DSA) Course; and
- Management Workstation Product (MWS) Course.

Network Security: As the number of users grows, the need to provide Network System Security (NSS) products increases. Today's information system communications environment consists primarily of dedicated system high networks—networks that are classified at the highest level of data they carry.

Communications between these different system high networks is limited. The goal with the deployment of NSS products is to eliminate dedicated communications backbones by collapsing them onto one unclassified backbone which will then carry data of different classification levels. Deployment of NSS components is intended to provide information system users with a wide range of Information Systems Security (INFOSEC) capabilities within an acceptable risk environment. This deployment philosophy is based on the principle of risk management instead of risk avoidance.

The basic NSS components are FORTEZZA cryptographic cards, Certificate Authority Workstations (CAWs), firewalls (discussed later on in this section), Standard Mail Guard (SMG)/Secure Network Server (SNS), and In-Line Network Encryptors (INEs). Deployment of a combination of NSS products provides users with a multi-level security capability. NSS products provide the security features which will be implemented as part of DMS deployment.

Firewall: A firewall is a collection of hardware and software components that is placed between two networks to provide security services. All traffic that passes between the networks must go through the firewall. The security services, provided by a firewall, include access control, user authentication, and logging/auditing. Firewalls can also be used to restrict network services/applications. These network services/applications may include HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), and SMTP. The local security policy, in place at the site, is the governing factor which defines what traffic will be allowed to pass through the firewall.

Some of the benefits of having a firewall are that it centralizes security management, allows for auditing, and it can be hosted on standard workstation platforms. FORTEZZA is currently being implemented within firewalls to provide stronger authentication mechanisms. A firewall, in itself, should not be viewed as a total security solution for networks. A combination of other NSS components should also be installed to reduce network vulnerabilities.

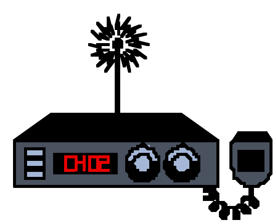
DMS will be explored in greater detail for the Interoperability Section later in this chapter

4.3 Mobile Communications

The wireless communications market is entering a period of long and steady growth. The technologies are yielding faster performance, there are more users than ever, and there are more available products. Many information technologists are beginning to augment their current LANs and WANs with some form of wireless data communications. This Section will focus on mobile communications technologies, and identify several alternatives which may meet all, or some portion, of the Coast Guard’s current and future communications requirements.

Wireless networks offer service to mobile assets and portable users. Wireless networks are usually the sole means for moveable platforms to communicate off-platform when on the move. Several wireless networking alternatives, including High Frequency (HF) and Satellite Communications (SATCOM) point-to-point communication technologies and services, are discussed below. A detailed analysis of three selected network alternatives will be conducted in Chapter 5.

4.3.1 Spread-Spectrum Packet Radio



In 1985, the Federal Communications Commission (FCC) allocated three frequency bands for a radio transmission technique known as Spread Spectrum communications, originally developed by the military. This transmission technique has much greater immunity to interference and noise compared to conventional radio transmission techniques. In addition, an increasing number of users can use the same frequency (similar to cellular). These rules are designed to drive usage towards local data communications.

The conventional radio signal is referred to as narrow-band, which means that it contains all of its power in a very narrow portion of the radio frequency bandwidth. Due to the relatively small portion of the radio band that an individual radio transmission occupies, the FCC has traditionally favored these conventional radios. However, as a result of the very narrow frequency, these radios are prone to interference (a single interfering signal at or near their frequency can easily render the radio inoperable).

Spread Spectrum is a technique that takes a narrow-band signal and spreads it over a broader portion of the radio frequency band. This has the operational advantage of being resistant to interference. However, due to unfounded concerns over the increased frequency space it occupies, the FCC, until recently, did not permit commercial use of the technology.

In performing Spread Spectrum, the transmitter takes the input data and spreads it in a predefined method. Each receiver must understand this predefined method and despread the signal before the data can be interpreted.

There are two basic methods to performing the spreading: (1) Frequency Hopping, and (2) Direct Sequencing. Frequency hopping spreads its signals by "hopping" the narrow-band signal as a function of time. Direct sequencing spreads its signal by expanding the signal over a broad portion of the radio band.

The FCC allows the use of Spread Spectrum technology in three radio bands, 902-928 MHz, 2400-2483.5 MHz and 5752.5-5850 MHz for transmission under 1 Watt of power. This power limit prevents interference within the band over long distances.

Spread spectrum is highly secure. Would-be eavesdroppers hear only unintelligible blips. Attempts to jam the signal succeed only at knocking out a few small bits of it. So effective is the concept that it is now the principal antijamming device in the U.S. Government's MILSTAR defense communications satellite system.

- **Advantages to Spread Spectrum:**

  - No FCC Site License - The FCC will grant a one time license on the radio product. After that license is granted, the product can be sold anywhere in the U.S.
  - Interference Immunity - Spread Spectrum radios are inherently more noise immune than conventional radios. Thus they will operate with higher efficiency than conventional technology.
  - Multi-Channel - Conventional radios operate on a specific frequency controlled by a matched crystal oscillator. The specific frequency is allocated as a part of the FCC site license, and the equipment must remain on that frequency (except for very low power devices, such as cordless phones).
  - Spread Spectrum data radios offer the opportunity to have multiple channels which can be dynamically changed through software. This allows for many applications, such as repeaters, redundant base station, and overlapping antenna cells.

A major point in choosing Spread Spectrum is the fact that you can implement a Code Division Multiple Access (CDMA) system which is a way of allowing more users to communicate at the same time in the same frequency band. Each user has its own code, therefore a message can be recovered knowing the right code. CDMA is able to "prioritize" signals based on the length of the code assigned. As the channel gets full, signals with shorter code lengths drop out first due to noise of other signals. CDMA is often considered the technology of choice because of its capacity and voice quality. The major advantage of CDMA is that it allows the provider to operate both fixed and mobile systems using the same infrastructure and platform. Currently, the high cost of CDMA makes it less attractive, and a large channel allocation is required. However, a rapid decline in equipment costs is expected, as cellular and other applications use drives up CDMA modem production.

The system is a short distance wireless communications system, whose application can be voice transmission, modem application, remote sensing/controlling, etc. The idea is having a point-to-point (non-cellular) system which does not need a complicated infrastructure. This system may serve as a reliable link for short-haul disaster communications and a critical component of the Transportable Communications Central (TCC) communications suite.

Table 4-6: Spread Spectrum Pros and Cons

PROS	CONS
Transmission Security	Limited to 1 Watt power
No FCC site license required.	Limited number of frequencies available.
Higher efficiency than conventional technology	Susceptable to Far-Near effect
Interference resistant	
Multi-channel capabilities	

(Note: The "Far-Near" effect is a problem which is caused by the fact that transmitters are received with non-equal powers. If, for example, there are three users in a specific cellular area, user-1 is transmitting traffic to user-2. It is possible that user-3 will interfere with User-2's reception if User-3 has more power and is closer to User-2 than User-1. In a cellular approach, this is addressed with the concept of Power Control. Frequency Hopping is another method of combating the Near-Far effect.) (Ref: http://www.eng.usf.edu)

Below is one example of how Spread-Spectrum technology is currently being used as a wireless network to route packets to and from mobile users.

- ***Ricochet Wireless Network:*** A good example of Spread-Spectrum technology is the Ricochet Wireless Network, which is a packet radio network operating in the unlicensed 902-928 MHz band. The technology requires a subscriber device and pole top repeating radios, Wired Access Points (WAPs), and Network Interconnection Facilities. Applications that operate using a wired modem for communications can become wirelessly enabled by replacing the phone modem with a Ricochet wireless digital modem. The modem is portable, weighing 13 ounces, and attaches to the serial port of any computer.

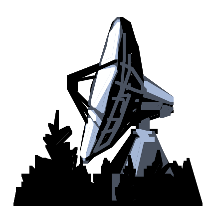
Repeaters are typically mounted on street light pole tops. The wireless mesh serves to route packets to and from mobile users. Interspersed amongst the mesh radios are WAPs. These are locations where the wireless packets are routed onto Ricochet's wired backbone. Once on the wire, the packets can be delivered via several means, including INTERNET.

Frequency hopping, dynamic routing, and password and authentication techniques make detection and interception of information extremely difficult.

The Ricochet LAN Gateway is installed on a user premises between a LAN and the Ricochet "cloud". Ricochet users can easily dial into the gateway wirelessly, providing they have been given the proper access privileges. Industry-standard encryption and authentication schemes ensure privacy for both the information transmitted and the access to the network itself. Depending on the Gateway's configuration and the wireline connection to the Gateway, it can support 100-1000 users. The Gateway provides "persistent connections" rather than the typical "continuous reconnections" required in a modem bank. For users, this means that, unlike traditional telephone modem banks, users will not get a busy signal when the number of users exceeds a certain number. Instead, the Gateway will provide equivalent performance for all users on the network, although the highest level of performance may not always be attained for individual users during peak usage periods.

Ricochet modems can be leased for $10 per month or purchased for around $200. The basic monthly service charge is $30, which includes unlimited wireless INTERNET access and a Post Office Protocol (POP) e-mail account. Telephone modem access capability can be added for another $5 per month, which gives you the ability to call into services accessible only through telephone numbers. Dial-in service, to allow you to retrieve mail from outside the Ricochet service area, is $10 per month. (Ref: http://www.metricom.com/ricochet)

4.3.2 Satellite Communications



Several commercial and military satellite systems are capable of meeting the Coast Guard's ever increasing record message and tactical communications requirements. The desire to "move data" more rapidly and with greater reliability drives the need to seek new and improved technology. This sub-section will discuss several currently available satellite communications technologies that may effectively meet the Coast Guard's current and future telecommunications requirements. Some of these technologies, however, are relatively new and have not yet matured into fully developed systems.

4.3.2.1 Low Earth Orbit Satellites (LEOS)

There are several satellite systems in various stages of development that may meet the Coast Guard's voice, data, and video communications requirements. These systems will greatly expand the available coverage areas by offering service everywhere on earth, including the polar regions where current satellite services cannot reach. LEOS will also eliminate the requirement for stabilized dish antennas for mobile platforms.

LEOS provide services as diverse as worldwide paging with acknowledgment, worldwide handheld telephone service, and vehicle tracking where the mobile unit sends up a continuous stream of information about its whereabouts. The primary advantage of LEOS is that the transmitting terminal does not have to be very powerful. The reason for this is that LEOS are so much closer to the earth than traditional geostationary satellites, which are satellites placed in a geosynchronous orbit 22,300 miles directly over the earth's equator. However, to maintain communications, you must always have "several" of these satellites above you.

There are several proposed LEO systems under development. These include Iridium, Globalstar, Odyssey, INMARSAT-P, Spaceway, and Teledesic. Because of big industry backing, Iridium and Globalstar are the two systems most likely to succeed.

- **<u>Iridium</u>**: Iridium is Motorola's satellite project to "bring personal communications to every square inch of the Earth." Although the project is still in the research and development stage, Motorola intends to provide global personal satellite based communications via handheld terminals by the year 1998. For the first time, anyone, anywhere, at any time can communicate via voice, data, or video. Motorola estimates the service costing approximately $3.00 per minute.

  The idea is that everyone will carry an Iridium handset no larger than today's cellular phone, and will be able to talk directly from their phone to the satellite (one of 66 satellites which will fly in eleven nearly polar orbits (tilted 86 degrees) 420 miles out) and then down to the ground or to a satellite dish, through landlines to the phone of the person being called. The benefit is that the system knows who you are and where you are the moment you turn on your phone. This feature may have several other uses in the maritime community, especially in the areas of SAR and law enforcement operations.

  The Iridium satellites will not only talk to handsets and ground stations, they will also talk to each other, forming a network aloft, passing on conversations, and handing them off when they drift out of range. Because of these satellite-to-satellite crosslinks, the Iridium system will be able to handle calls to other Iridium phones without reference to any ground stations at all, once the link is established.

Iridium's primary features include:

— A constellation of 66 satellites in a low Earth orbit of 483nm;

— Satellites travel 15,000 mph, circling the earth once every 100 mins.;

— 11 operational satellites and one spare will populate each of 6 orbital planes;

— 48 spot beams within each satellite's footprint;

— A 16db signal power margin, enabling customers to use the handset inside a car;

— A 5 to 7 year on-orbit lifetime;

— Both frequency and time division multiplexing;

— Digital voice at 4.8kbps, and data at 2.4kbps;

— 15 to 20 ground gateways that link the satellite system with the terrestrial public switch telephone network; and

— A master control center in the U.S. and a backup facility in Italy.

(C4I Technology Assessment, Pg. 110-111)

- **<u>Globalstar:</u>** A new communications tool—the hand-held satellite telephone—will be available before the turn of the century. At about the same time, affordable, basic telephony—through fixed-site satellite telephones—will be available for the first time. Globalstar will usher in both.

  Globalstar is a LEO satellite-based digital telecommunications system that will offer wireless telephone and other telecommunications services worldwide beginning in 1998. Globalstar will provide low-cost, high quality telephony and other digital telecommunications services, such as data transmission, paging, facsimile, and position location to areas currently underserved or not served by existing wireline and cellular telecommunications systems.

  Globalstar service will be delivered through a 48-satellite LEO constellation that will provide wireless telephone service in virtually every populated area of the world. Globalstar will begin launching satellites in the second half of 1997 and will commence initial commercial operations via a 24-satellite constellation in 1998.

  Full 48-satellite coverage is projected for the first half of 1999. Users will make or receive calls using hand-held or vehicle-mounted terminals, similar to today's cellular telephones. Because Globalstar will be fully integrated with existing fixed and cellular telephone networks, Globalstar's dual-mode handsets will be able to switch from conventional cellular telephony to satellite telephony, as required.

In remote areas, with little or no existing wireline telephony, users will make or receive calls through fixed-site telephones, similar either to phone booths or ordinary wireline telephones. Each subscriber terminal will communicate through a satellite to a local Globalstar service provider's interconnection point (a gateway) which will in turn connect into existing telecommunications networks.

Hand-held and mobile services will be provided to areas where cellular coverage is poor or non-existent. Users will include fishing boats, yachts, and other small craft and short-haul commercial and general aviation aircraft.

Telecommunications service providers AirTouch, Dacom, France Telecom, Elsag Bailey, and Vodafone will provide on-the-ground marketing and telephony expertise to Globalstar. Telecommunications equipment and aerospace systems manufacturers have contracted to design, build, and deploy the Globalstar system. Loral Corporation has overall management responsibility for the Globalstar system, its design, construction, deployment, and operations. Loral will build Globalstar's satellite operations control centers (SOCCs) and portions of its ground operations control centers (GOCCs).

Qualcomm, Inc., using its CDMA technology, will design and manufacture subscriber terminals and gateways, and will have primary responsibility for the design and manufacture of the GOCCs.

To achieve low cost, reduce technological risk, and accelerate deployment of the Globalstar system, Globalstar's system architecture uses small satellites incorporating a well established repeater design that acts essentially as a simple "bent pipe," relaying signals received directly to the ground.

(POC: Globalstar Limited: (408) 473-5872)

4.3.2.2 American Mobile Satellite Corporation (AMSC)

AMSC provides satellite-based mobile voice and data communications services throughout the United States. Their satellite telephone service provides a variety of land, maritime, and aeronautical based applications. Pleasure boaters, commercial mariners, and government can subscribe to satellite service to gain access to ubiquitous mobile telephone services hundreds of miles off U.S. shores. However, ships at sea will need the stabilized dish antenna because they will be operating on the fringe areas of the satellite's effective footprint. This service is available at a fraction of the cost of satellite telephone services offered today by other companies.

AMSC terminals are small and inexpensive, and their charge per minute is reasonable. This will allow installations on most Coast Guard vessels, and AMSC covers the vast majority of the areas where the Coast Guard operates (i.e., virtually all of North America, the Caribbean, and all U.S. coastal waters). Voice, data, and FAX will be available, and a Global Positioning System (GPS) chip will allow location to be displayed on the handset. Differential GPS corrections are available over the satellite. AMSC provides fixed site support for remote locations and for alternate routing for high priority circuits where landlines may be vulnerable to terrestrial disasters.

AMSC will provide normal telephone service, from your mobile satellite unit, at rates a fraction of those currently available elsewhere. With AMSC, there are no additional long distance charges for domestic calls.

STU-III, as well as other NSA approved secure data and voice systems will be available. This will allow alternatives for Navy Fleet Satellite Communications (FLTSATCOM), High Frequency Data Link (HFDL), and other systems where a secure capability is necessary.

AMSC also has a low cost aeronautical terminal. The Coast Guard is currently testing some of these terminals on HH-60 helicopters. They will provide an alternative for long range aeronautical communications.

The AMSC system allows for "talk groups" to be established. These may be used for messages or party line applications. For example, all cutters in the Caribbean could constitute one talk group, oil spill responders another, etc. All maritime users in an area could be in a talk group for facilitating maritime safety and receiving marine information broadcasts. Each telephone may belong to a maximum of 15 different talk groups, and each talk group may have as many as 10,000 phones.

Talk groups may be reconfigured over the air, when necessary, without local operator intervention. This will be ideal for establishing interoperability during an emergency when units of several different organizations respond. (If this were implemented in the short term, there would be a giant leap toward interoperability and emergency support.) Many different organizations at the Federal, state, local, and emergency response level are currently using the AMSC system. For the first time, interoperability among all organizations is possible.

Access to the Public Switched Telephone network (PSTN) via the AMSC gateway in Reston, Virginia allows for operations during periods when systems in the area of an emergency are stressed. When hurricanes or earthquakes occur, the AMSC satellite will be above it all and unaffected.

Key attributes of the AMSC satellite system include signal intelligibility and clarity.

Dual mode satellite/cellular radios cost about $3,000; per minute charges for government organizations are $1.20 or less, including terrestrial long distance charges. Talk groups can be established for $100 per month, and practically unlimited users may join them for $70 per month. The $70 per month allows dispatch and significant talk time for users. The Coast Guard could buy 1000 radios for $3 million and operate them in 100 talk groups for about $80,000 per month. Studies have shown that up to 35 users per circuit can be accommodated, so 100 talk groups per 1000 users is conservative.

(POC: Kelly Dressler, AMSC, 10802 Parkridge Blvd. Reston, VA 22091)

4.3.2.3 International Maritime Satellite (Inmarsat)

INMARSAT commenced formal operations on 1 February 1982. The Communications Satellite Corporation (COMSAT), Washington, D.C., is the sole U.S. representative in the INMARSAT Organization, an international organization with 66 member countries that is headquartered in London, UK. COMSAT operates several INMARSAT earth stations in the U.S. and overseas. INMARSAT-A terminals are installed on cutters (210 WMECs and larger), and are used to support both voice and data communications. INMARSAT-C terminals are currently being installed on 110 WPBs and larger cutters, and are capable of data communications only. INMARSAT-A can be used for secure communications, if operated with appropriate cryptographic equipment (i.e., STU-III). Both “A” and “C” terminals are capable of receiving INMARSAT SafetyNet broadcasts, which is a service of the Global Maritime Distress and Safety System (GMDSS) for disseminating maritime safety information to ships on the high seas. Terminals now cost $45,000 each and are as big as file cabinets. Even the newest, briefcase-size model costs $25,000, plus $5.50 per minute of use.

INMARSAT is capable of meeting Coast Guard voice and data requirements, and is generally considered more reliable to use than most of the traditional methods of short, medium, and long-range communications. However, INMARSAT is significantly more costly to operate, with current usage charges of approximately $5.50 per minute. In time, costs are expected to decline as other commercial satellite systems are brought on-line, but under the current budget climate, the Coast Guard has elected to take an active approach to finding a less costly alternative. They are currently testing other satellite systems, in an effort to decrease operating costs and increase the availability of satellite communications.

INMARSAT wants to get into the handheld business, but hasn’t yet decided just how it wants to go about it. The idea has a name—Project 21—and INMARSAT has commissioned studies by a number of major companies for it. With 66 governments on its side, geostationary satellites already in place, and a rapidly growing cash flow from its existing operations, INMARSAT could end up with a global monopoly on satellite phones (in combination with AMSC).

Table 4-7, below, summarizes the characteristics for Iridium, Globalstar, AMSC, and INMARSAT mobile satellite systems.

Table 4-7: Commercial SATCOM Characteristics

Item	Iridium	Globalstar	AMSC	INMARSAT
Satellites	66	48	3	4
Altitude	483.3 miles	750 miles	22,000 miles	22,000 miles
Orbits	Circular 860 tilt	Circular 520 tilt	Geostationary	Geostationary
Uses	Mobile voice, fax, paging	Mobile voice, fax, e-mail	Voice, data, fax, messaging, position location	Voice, data, fax, paging, messaging, position location
Antenna Size	2 meters	1 meter	6.5 meters	1 meter
Spectrum Sharing	No	Yes	Info. Not Avail.	Info. Not Avail.
Modulation Scheme	TDMA	CDMA	Info. Not Avail.	Info. Not Avail.
Intersatellite Links	Yes	No	Info. Not Avail.	Info. Not Avail.
Turnkey	1998	1998	Currently Available	Currently Available
Price per minute	$3.00	$0.30	$1.50	$6.00
Initial Cost	$3,000.00	$700.00	$3,000.00	$25-45,000
Data Speed	4.8kbps	4.8kbps	2.4kbps	2.4kbps
Mode	Satellite	Satellite	Satellite/Cellular	Satellite
Coverage	Global	Global	N. America, U.S. coastal waters, Caribbean, Gulf of Mexico	Global
Voice	Yes	Yes	Yes	Yes
Data	Yes	Yes	Yes	Yes
Handheld	Yes	Yes	Yes	Yes
Mobile	Yes	Yes	Yes	Yes
Fixed Site	Yes	Yes	Yes	Yes

4.3.2.4 Very Small Aperture Terminal (VSAT)

VSAT networks provide rapid and reliable satellite transmission of data, voice, and video between an unlimited number of geographically dispersed sites or from these sites to a central site. Each site is equipped with a VSAT terminal consisting of an antenna, outdoor electronics mounted on the antenna for signal reception/transmission, and indoor electronics for connection to the computer terminal, telephone, and video equipment.

There are three standard VSAT network configurations: (1) Point-to-point, which provides two-way communications between VSATs located at two remote sites. Ideal for point-to-point links over large distances and in hard-to-reach locations, as well as for complete backup of vital network links; (2) Star network, which provides multipoint communications between a hub station located at the central site and VSATs located at an unlimited number of remote sites; and (3) Mesh network, where there are direct communications between VSATs at all sites on the network. Communications are not routed through a hub station; each site on the network "talks" to the other sites with a single satellite hop. Ideal for voice links to hard-to-reach locations, and for data communications among a smaller number of remote sites.

In Section 4.2.6, we described VSAT as a viable shore unit data networking alternative. In the future, a VSAT alternative will apply to mobile units as well. As with shore unit communications, this new and emerging technology will offer cutters high speed access to the INTERNET via a digital satellite system. Large files can be transferred at 3 Mbps, with full broadcast channel capacity of 12 Mbps. This system also offers Digital Encryption Standard (DES) compatibility.

Low cost commercial two-way VSAT networking is well into the developmental stage, and maritime mobile VSAT technology has been demonstrated as well. For these reasons, a VSAT network may soon be expandable to most Coast Guard mobile units. The lack of single point failure commonality with the terrestrial networks, should provide major advantages of reliability and survivability either as a back-up or primary system.

Several service providers offer the technically advanced, user-friendly satellite communications products. These include:

- **AT&T Tridom:** AT&T's Tridom provides VSAT systems to government agencies and communications service providers throughout the world. Using Time Division Multiple Access (TDMA), Tridom connects remotely located computer terminals to the satellite network. The VSAT system includes a network interface unit (NIU), a small antenna and outdoor unit that receives and transmits the satellite signals, and a hub station that contains the central switching and transmission equipment to link all parts of the network.

  A router offers one of the first LAN-capable VSATs that allows users with Ethernet LANs, based on TCP/IP, to interconnect directly with a VSAT-based WAN. The Internet Protocol (IP) router supports communications between any two points on the network. A user can access data located locally, on a remote LAN or in the central host computer. The IP router's diverse capabilities include the ability to route data via terrestrial lines between overloaded sites and the hub, thereby simplifying network management. The IP router's full compatibility and flexibility simplifies operations.

  A voice link module is a compressed digital voice option that allows you to have two-way voice communications on the VSAT networks. The module enables the voice link to share the same outroute and inroute as the data link, thus providing a cost-effective alternative to terrestrial systems and expanding the capability of the VSAT network.

  The Tridom Demand Assigned Multiple Access (DAMA) system represents the state-of-the-art demand-based satellite networking. The DAMA system provides stand-alone connectivity, redundancy, and supports various demand-based connections. With the DAMA system, each terminal can communicate with one or more terminals directly through a single hop link. This intelligent system utilizes sophisticated network control systems and advanced communications technology to provide clear communications access to all subscribers. It is best suited for peer-to-peer voice and data communications in a full-mesh topology where switched circuits are needed and single satellite links are essential.

The new AT&T Global VSAT systems come in two basic models, the Clearlink System 200 and the Clearlink System 400. The two VSAT systems operate with either private or shared hub earth stations, and both models use the Clearlink NIU, which is programmed for either Ku- or C-band transmission.

The smaller system, System 200, is a Ku-band VSAT designed primarily for North American customers with low-volume data traffic who want the flexibility of low-cost satellite data communications. The System 200 uses the smaller 0.95 meter antenna and provides a fixed 64kbps inroute data rate and 256kbps outroute rate.

The versatile System 400 is available in both Ku- and C-band models. The model takes full advantage of the unique software programming capability to provide greater flexibility in network delivery to match changing traffic requirements. Software-programmable variable transmission rates means that the System 400 network can be initially deployed with an inroute data rate of 64kbps and an outroute speed of 128kbps to minimize space segment costs, and then, as traffic demand increases, be re-configured to operate at higher outroute rates of either 256kbps or 512kbps. And, because it is all done by software, the upgrade can be done by the Coast Guard with no additional hardware and no site visits, minimizing the costs. The System 400 can be installed with either a 1.2, 2.4, or 3.5 meter antenna, depending on geography and network configuration.

Both Systems are fully compatible with digital compression and AT&T's new Skynet Global Video Service, which provides compressed digital video satellite transmission. In addition, the System 400 is compatible with the Clearlink Ethernet Router Option (ERO), a plug-in interface card that provides connectivity to 802.3 Ethernet LANs through TCP/IP software. The System 400 also has a compressed digital voice option in the new Clearlink Voice Link Module, which provides cost effective two-way voice communications on VSAT networks.

Prices for the System 200 range from approximately $6,000 to $9,000 per VSAT and the System 400 ranges from approximately $10,000 to $25,000 per VSAT, depending on satellite frequency band and antenna size.

(POC: bob.proffitt@tridom.com)

- **<u>DirecPC:</u>** DirecPC, as discussed in Section 4.1.6, is a data networking alternative that has the potential to meet several Coast Guard communications requirements, including providing voice, data, and video service to mobile units.

  There are three main types of DirecPC service that may be offered: (1) Package Delivery; (2) MultiMedia; and (3) Turbo Internet. Broadly stated, Package Delivery is used when the destination of the information is storage; MultiMedia for "live" broadcast of information; and Turbo INTERNET for INTERNET access and download of files at much higher than dial-up modem rates.

— *Package Delivery:* DirecPC Package Delivery service provides one-way broadcast of digital video, audio, or text based files, such as software, computer-based training, documents, or any other content from a central site to any number of locations. The broadcast can be either scheduled or on demand.

— *MultiMedia:* DirecPC offers one-way packet transmission in a "data-pipe" format for video, audio, or regularly transmitted information that is scheduled and provided as a service. This service is available to a selected group, or all of an information providers locations. The transmission schedule can be selected to meet the needs of the organization, such as:

  - Fixed duration (example - 2 hours per day, every Monday at 1 p.m.);
  - Dynamic; and
  - Continuous streaming of audio, video, or high speed data.

  A conditional access mechanism ensures that a receiving unit may only access data of which the Network Operations Center (NOC) has individually authorized it to receive. The NOC architecture has been made scaleable and broadcast capacity is allocated based on the broadcast provider's Committed Information Rate (CIR).

— *Turbo INTERNET:* Turbo INTERNET access allows terminals to be connected to the INTERNET via DirecPC (for packets from the INTERNET) and dial-up model (for packages into the INTERNET). The NOC is connected to an INTERNET Access Provider (IAP) by terrestrial line. The NOC is also connected to the PSTN by a terminal server. Currently, the DirecPC users must either dial into the NOC or into an existing IAP. In the future, mobile users may be able to access the NOC by other means.

As with any telecommunications system, timing is a critical base technology and protocols are enabling/limiting factors. Electronic data can take as long as half a second to travel up and down to Earth from geostationary satellites, which are positioned 25,700 miles away from the planet. Although a delay of that magnitude causes only a slight echo when placing a telephone call, it can wreak havoc when two computers are trying to communicate. The delay causes TCP/IP to believe there is a backup in the network, which in turn disrupts the electronic acknowledgments the receiving computer must relay to the sending computer in order to confirm that messages are being received correctly. Hughes DirecPC works around this limitation by permitting the user to send requests for data directly to the INTERNET by modem. The requested information from the INTERNET flows to back to the Hughes NOC. At the NOC, the data is spooled and the IPA is spoofed. (This provides a larger, more effective TCP window size.) The NOC transmits the data via the Direct Broadcast Satellite (DBS) to the DirecPC VSAT user's computer.

In the near future, DirecPC service will widen its offer to include service to what is known as the Enterprise. DirecPC will then also be installed in servers as well as in standalone PCs. A server based platform extends DirecPC service across the LAN and evolves its current capability of automatically transferring files to the server as they arrive on a separate platform than that of the destination server.

DirecPC's (Hughes') satellite, the Galaxy IV, is a member of the dual-payload, three-axis, body-stabilized HS601 family of spacecraft. It is located at 99 West longitude and provides a variety of satellite services, over 24 channels, to users in the continental U.S., Alaska, Hawaii, and Puerto Rico. Hughes has announced future plans to combine DirecPC and DirecTV systems into one consumer product using one dish. The DirecPC dish will be able to receive the DirecPC signal from Galaxy IV and also from a neighboring DBS satellite broadcasting the DirecTV signal.

Currently, package costs range from $15.95/month plus $.60 per Mb to about $170-200 per month unlimited 24-hour access. A DirecPC access kit costs approximately $899.00 for basic access service only, and $1349.00 for basic access service and the license to receive broadcast services.

Table 4-8, below, shows the components and cost of a typical DirecPC installation. Actual cost may vary depending on the service provider selected.

Table 4-8: DirecPC Facts/Costs

System Requirements	DirecPC Access Kit	Installation	Turbo INTERNET Service
PC w/Pentium Processor	21" Elliptical Dish	Do it yourself = $0	One-time Activation Fee = $49.95
Windows '95	100' of coaxial cable	Ground Mount = $99	Monthly Access Fee = $9.95/mo.
16 Mb of RAM	16-Bit ISA Card	Roof/Wall Mount = $149	Night Surfer Plan = $39.95/mo.
20 Mb free hard disk space	Turbo INTERNET Software	Custom Install = $89/hr.	Day Surfer Plan = $129.95/mo.
Modem (9600 baud or better)	DirecPC Installation		Bulk Plan = 24.95/mo.
A clear line of sight South	DirecPC Users Manuals		Basic Plan = $.60/Mb

(POC: http://www.direcpc.com)

- **Direct Broadcast Satellite:** In the early 1980s, the Federal Communications Commission (FCC) approved the use of commercial broadcast satellites to deliver television broadcasting directly to home receivers, thus bypassing standard commercial television stations and cable operators. The FCC calls this new class of television service "Direct Broadcast Satellite" (DBS). In April 1993, the Navy requested a proposal to demonstrate the feasibility of the new DBS capabilities to support Naval operations and to solve some of the Navy's communications problems. The project was known as "Radiant Storm" and the tests concluded that:

- High data rates can be easily achieved using DBS;
- High power satellite transponders are necessary for military communications in the future;
- High power transponders make VSATs and high data rates possible;
- Encryption works with commercial DBS technology; and
- Very low error rate channels are possible.

A shipboard demonstration of DBS was done in November 1994. This effort was a demonstration of the television capability and did not transfer military data. Ship personnel reported that DBS exhibits outstanding signal quality and interference free operation. The potential exists for near perfection when and if antenna stabilization improvements are made.

Within the military, there is considerable interest in DBS technology. At this time, a military Global Broadcast System (GBS) system is in development, and it should be operational within the next two years. This new GBS will complement, if not replace, the use of Fleet Broadcast for the Navy. The Coast Guard could benefit from the planned GBS, because some, if not most, of the data to be provided by GBS is also required by the Coast Guard. Additionally, the terminal equipment required to receive the GBS is both small in size, including a very small diameter antenna (less than 1 meter) and inexpensive in cost. The data of interest will consist of:

- Warnings;
- Common tactical picture;
- Weather maps and forecasts;
- Theater chart updates;
- Intelligence updates;
- Message traffic; and
- News broadcasts.

Full operational capability is expected by the first quarter of 1999. Until the Full Operational capability is achieved, a Phase I GBS system has been implemented with the one year lease of a high data rate Ku-band transponder on the communications satellite Telstar 402. There is a GBS Phase I user hardware suite that includes a 1 meter dish, a commercial receiver, a rate buffer module that provides the data interface to a user's computer equipment, and a KG-194 cryptographic unit. The cost for this hardware suite is roughly $40,000.

The Navy accomplished a technology demonstration showing high rate data communications (T1) to littoral platforms. In the demonstration, a T1 data rate was achieved to a buoy using a commercial (Seatel) VSAT modified for transmission as well as reception using off-the-shelf commercial components. One of the most interesting aspects of this demonstration was the integration of current cellular CDMA technology. This should allow better use of the available bandwidth from a commercial satellite video channel, potentially up to 30 T1s per channel. This technology should have potential for Coast Guard applications. (C4I Technology Assessment Pg. 95-96)

4.3.2.5 Military Satellite Communications (MILSATCOM)

The mission of MILSATCOM is to provide a survivable, command and control communications system to meet the projected minimum essential wartime operational requirements associated with military communications. In September 1978, the Navy announced a contract award to Hughes Communication Services, Inc., to provide worldwide communications satellite service to DoD. The first satellite was successfully launched in August 1984. Currently, the Navy UHF Fleet Satellite Communications (FLTSATCOM) system consists of a combination of leased and Navy owned satellites that provide world-wide communications connectivity with naval ships and airborne platforms. The FLTSATCOM system comprises space, earth, and control segments. Space and earth segments consist of satellites, earth terminals, subscribers, and subsystems.

As stated in Chapter 2, Coast Guard assets have access to certain MILSATCOM systems based on unique operational requirements and interoperability needs with the Navy. Larger cutters (378 WHECs and 270 WMECs) and some smaller cutters (210 WMECs) are equipped with FLTSATCOM capabilities. FLTSATCOM subsystems most commonly used by Coast Guard units are OTCIXS, CUDIXS/NAVMACS, and FLTBROADCAST (see Chapter 2 for additional information on these systems).

The MILSATCOM system is divided into three general types of communication systems, depending on the frequency range in which the transceiver subsystem operates. These systems are:

- **Ultra High Frequency (UHF):** The UHF satellite system provides communications between suitably equipped mobile units and shore facilities. These links supply worldwide coverage between the latitudes of 70 degrees North and 70 degrees South. The FLTSATCOM system is also deteriorating and is being incrementally replaced by the UHF follow-on (UFO) satellite system. At this time, there are five UFO satellites in orbit and four additional satellites scheduled to be launched. The Coast Guard uses Demand Assigned Multiple Access (DAMA) UHF satellite equipment suites on several classes of ships now. These classes are: 378’ WHECs, 270’ WMECs, most 210’ WMECs, and WAGBs. In addition, the 210’ WMECs, currently equipped with non-DAMA SATCOM, are scheduled to receive DAMA SATCOM capabilities during FYs 97-98.

- **Super High Frequency (SHF):** The SHF spectrum is a highly desirable SATCOM medium because it possesses characteristics absent in lower frequency bands, such as wide operating bandwidth, narrow uplink beamwidth, anti-jam, and relatively high data rates. The actual ship-to-shore SHF satellite links are provided by the Defense Satellite Communication System (DSCS). The DSCS is an integral part of the Defense Communications System (DCS), designed to provide vital worldwide communications service to the U.S. and NATO/Allied Forces via satellite.

- **Extremely High Frequency (EHF):** The EHF system provides essential tactical and strategic communications services. It incorporates multiple design features that provide low probability of intercept, anti-jam, survivable, and enduring military communications capabilities. It is designed to meet the minimum essential command, control, and communications requirements of the National Command Authority and strategic and tactical military forces. MILSTAR (Military Strategic, Tactical and Relay) is the name given to the program that developed the use of the EHF frequency band for military SATCOM. Under the MILSTAR program, both space and ground segments of the system were developed. Currently, the term MILSTAR and EHF are used interchangeably when referring to the military EHF communications system. The shipboard terminal also uses one or two antennas. Because of the relatively large physical size of a MILSTAR terminal, its use would not be practical on all but the largest of the Coast Guard ships. An even more important reason that MILSTAR use is not likely for the Coast Guard is the same as the reason that restricts Coast Guard use of UHF and SHF, namely low requirements priority.

Other MILSATCOM systems/technologies include:

- **Military Global Broadcast System (GBS):** This system, currently under development, will use the DSCS to provide GBS to the military using government owned space assets and currently used terminal hardware. The plan is to demonstrate the utility of such a system by moving some of the current UHF and SHF traffic onto the X-band GBS broadcast. The X-band system would provide a limited data rate Navy Broadcast capability. It would also require modfied SHF terminal hardware. The intent is to modify flights of the UFO program to include the high power wideband transponder for the GBS application. The first of these is scheduled to fly late 1997 or 1998. (See VSAT (DirecPC) for more details.) The operational concept is to have some bandwidth set aside for general broadcast (producer-push) similar to Tactical Related Applications Broadcast and Fleet Broadcast (the first two world-wide broadcast systems) and some for query services (user-pull) response. The actual data format is being defined as the frequency of the broadcast with the SHF (X-band) favored over the Ka-band (20 gHz). During recent joint Navy/Marine Corp. tests, data was transmitted over the commercial DBS satellite at a 23 Mbps data rate. Several types of data, mostly tactical intelligence, were successfully transmitted.

- **UHF Demand Assign Multi-Access (DAMA):** This subsystem provides users with increased communications capacity and reliability over dedicated access on the FLTSATCOM satellites. The additional capacity is provided by the time division multiplexing feature of DAMA. DAMA is capable of multiplexing secure voice, record message, and data systems on a single 25kHz satellite channel. DAMA increased the capability of military communications links by time sharing each channel among multiple users. Icebreakers, High Endurance and 270ft Medium Endurance cutters have DAMA, while 210s and the Transportable Communications Centrals (TCCs) are being upgraded to DAMA.

- **Mini-DAMA:** Mini-DAMA is the solution to the UHF DAMA SATCOM requirements of small vessels and C3/surveillance aircraft performing naval or joint operations. Based predominantly on contractor-off-the-shelf (COTS) technology, Mini-DAMA achieves high reliability in a low-cost terminal for DAMA operations. It provides the following features:

  — Interoperability with existing Navy communications systems;

  — Time Division Multiple Access (TDMA)/DAMA for shared use of 5 and 25kHz channels on existing and planned satellite transponders;

  — Eight, full-duplex baseband I/O ports per communications set;

  — Embedded OTCIXS;

  — Simple, menu-driven, flexible operator interface;

  — Over-the-air and field modifiable software;

  — Embedded orderwire encryption; and

  — Multiple embedded COMSEC (ANDVT, KG-84, and KY-57/58) capabilities.

  (Ref: http://www.disa.atd.net/dama)

- **High Speed Fleet Broadcast:** The Navy is currently replacing its out-dated, slow speed (75 baud), multi-channel (16 channels HF/16 channels satellite) fleet broadcast, implemented in 1968, with a new High Speed Fleet Broadcast (HSFB). The HSFB will be capable of speeds of up to 19.2kbps. However, as currently planned, General Service (GENSER) and Sensitive Compartmented Information (SCI) message traffic will run at 2.4kbps, with a total throughput of 9.6kbps. The new HSFB will use a Mil-188-110 modem for HF and a CODEC modem for satellite communications. The HSFB is scheduled for installation on 28 Coast Guard cutters in the 1998-99 timeframe. (POC: LCDR Rohrbach, 703-695-7599)

- **Commercial Satellite Communications Initiative (CSCI)**: Commercial satellite use in the military is growing rapidly. DOD will have an extensive replacement program for satellite communications. Some of that program will be DOD-specfic for security reasons, but it is expected to rely heavily on commercial providers. DISA currently leases commercial transponders through its CSCI contract held by COMSAT (RSI). One visible project is the support of current U. S. Operations in Bosnia. Challenge Athena is another application underway.

(Ref: http://www.fcw.com)

- **Challenge Athena**: Challenge Athena is a commercial satellite (SATCOM) implementation to provide for high bandwidth (T-1 duplex) on carriers and other capital ships in support of intelligence gathering, medical, meteorology and morale and welfare services. This proof of concept prototype has successfully transmitted four radiological images from an aircraft carrier to a shoreside location via SATCOM. The project uses satellites owned by the International Telecommunications Consortium. Challenge Athena's success has encouraged the Navy to consider significant investment in high-data-rate communications to its ships via satellite. (Ref: http://www.matmo.org/pages/projects/navyproj.html)

4.3.3 Cellular Communications

Coast Guard units are demanding more sophisticated services to meet their mobile communications needs. Cellular telephone service can help meet customer needs through a choice of applications and advanced services that were previously available only to wireline subscribers.

4.3.3.1 Circuit-Switched Cellular Networks

The concept of a cellular radio network was first invented by Bell Laboratories back in 1947. It would be over 35 years later before technology caught up with the cellular concept and allowed the first analog networks and terminals to be manufactured.

Fundamentally, a cellular network comprises a series of low power base station sites, each providing a relatively small area of coverage which combines to form contiguous coverage throughout a given area. By employing these low power sites, it becomes possible to re-use frequencies on a more regular basis which provides greater overall capacity to the network.

The coverage provided by each base station corresponds to the number of users that are likely to exist between that area, which is called a cell. Hence, more densely populated areas demand smaller cells and the intelligent aspect of the network provides the ability to allow conversations to continue without interruption as subscribers move between these cells. The process whereby a conversation is passed from one cell to another is known as "hand-off."

There are over 23 million cellular subscribers around the world and about half of these exist in the U.S. The use of mobile phones is expected to double in the world's population of cellular subscribers before the end of 1997.

Communicating across circuit-switched cellular networks involves the use of a cellular phone for voice communications or attaching a wireless computer modem to a cellular phone for data communications. Connection via an air-link through a nearby cell, then through the regional switch and ultimately through the telephone network to another computer is continuous until the link terminates when one participant hangs up.

The existing analog cellular network has a huge installed infrastructure providing "seamless" coverage, but only moderate speed (slower than spread-spectrum technology or Cellular Digital Packet Data (CDPD)) and high cost (more expensive, for example, than spread-spectrum or satellite transmission). Transmission of data is billed by the minute rather than by the character or bits-per-second, in some cases yielding up to ten times the price of other wireless services to transmit identical quantities of data. The service offers access to the information services, like INTERNET, America Online, and CompuServe.

For an added cost, you can obtain improved signal-transmission reliability with error correcting protocols which will automatically adjust transmission speed and protect the data from interference.

The following cellular technologies, which are either currently under development or available on the market today, may now, or in the future, meet certain Coast Guard voice, data, and video requirements. (Technologies not currently available in the U.S. should be monitored for future availability.) These technologies may be discussed in greater detail in Chapter 5.

- **Universal Mobile Telecommunication System (UMTS):** The Universal Mobile Telecommunications System (UMTS) is a new technology, third generation portable communication system, currently being developed in Europe. Some requirements for UMTS are:

    - To support existing portable services and fixed telecommunications services up to 2 Mbps;
    - To support unique portable services, such as navigation, vehicle location, and road traffic information services;
    - To allow the UMTS terminal to be used anywhere, in the home, office, and public environment, both in rural areas and city centers; and to offer a range of transportable terminals from a low cost pocket telephone (to be used by almost anyone, anywhere) to sophisticated terminals to provide advanced

video and data services. (C4I Communications Technology Assessment Pg. 43)

- **<u>Global System for Mobile Communications (GSM)</u>**: The Global System for Mobile Communications (GSM) is a new technology, digital cellular communications system which has rapidly gained acceptance and market share worldwide, although it was initially developed in a European context. In addition to digital transmission, GSM incorporates many advanced services and features, including ISDN compatibility and worldwide roaming in other GSM networks. The advanced services and architecture of GSM have made it a model for future third-generation cellular systems, such as UMTS.

  The system meets the following criteria:

  - Good subjective speech quality;
  - Low terminal and service cost;
  - Support for international roaming;
  - Ability to support handheld terminals;
  - Support for a range of new services and facilities;
  - Spectral efficiency; and
  - ISDN compatibility.

  Commercial service was started in mid-1991, and by 1993 there were 36 GSM networks in 22 countries, with 25 additional countries having already selected or considering GSM. Although standardized in Europe, GSM is not only a European standard. GSM networks are operational or planned in almost 60 countries in Europe, the Middle East, the Far East, Africa, South America, and Australia. In the beginning of 1994, there were 1.3 million subscribers worldwide. By the beginning of 1995, there were over 5 million subscribers. (C4I Communications Technology Assessment Pg. 44)

  Primary advantages of GSM:

  - Increased radio spectrum efficiency to provide even greater network capacity (supports a high amount of subscribers);
  - Provides highly sophisticated subscriber authentication;
  - Prevents the eavesdropping of conversations by employing sophisticated voice encryption techniques which are totally secure;
  - Provides better voice clarity and consistency, emanating interference due to digital transmission (turns speech into binary numbers);

- Simplifies the transmission of data which allows the connection of laptop and palmtop computers to GSM cellular phones;
- A single standard allowing International Roaming between the world's GSM networks; and
- One phone - one number.

GSM networks operate in the frequency range 890-915/935-960 MHz by means of 140 duplex radio channels, each of which is 200 kHz in bandwidth. The frequency split between these two bands is 45 MHz which is also the bandwidth between the transmit and receive frequency of the GSM terminal.

A technique known as Time Division Multiple Access (TDMA) is used to split this 200 kHz radio channel into 8 time slots, each of which constitutes a separate voice channel. Unlike normal analogue signals, the transmission of a voice channel is not continuous. By employing 8 time slots, each channel transmits the digitized speech in a series of short bursts, each of which adds up to a total of one eighth of a second. Hence a GSM terminal is only ever transmitting for one eighth of the time.

The advantage of TDMA with its system of time slots is that you can re-use frequencies within a closer proximity as there is less probability of interference. This provides greater efficiency which, in turn, allows the accommodation of more users.

4.3.3.2 Cellular Digital Packet Data (CDPD)

CDPD, offered by several providers, including Tellabs Wireless Systems, uses the already well-established cellular phone network for wireless data transmission. This means that CDPD works on top of, or along side the cellular telephone system. CDPD uses the same radio spectrum as the cellular telephone system and can use the same radio engineering designs as the cellular telephone system.

The benefits of this approach to developing a wireless data network is twofold. First, it allows the device manufacturers to develop equipment based on proven radio technologies. Second, it allows the service providers to re-use much of their existing infrastructure. This is not to say that CDPD is all old technologies. In fact, CDPD is a digital system. It encodes all data into digital transmission bursts and transfers these bursts over the air efficiently. Part of this efficiency comes from using a forward error correction scheme in all data transmissions. By using forward error correction methods, there is a reduction in the need to repeat lightly corrupted data bursts. Retransmissions are only necessary when the data block is damaged beyond repair.

Another efficiency improvement comes from the recognition that CDPD is a data network. Data communications are typically bursty in nature. CDPD makes use of this characteristic by packetizing the data transmissions and allowing multiple devices to share the same radio channel. Orderly sharing of the channel is managed by the Medium Access Control scheme.

Coverage is currently minimal, but eventually should be identical to the existing cellular network. This may be years away. There is much debate among analysts as to when it will be fully operational. Service providers are in the early process of building the regional infrastructures and at the same time, are beginning to interconnect the separate regions into national network. The actual scale of CDPD adoption will be very dependent on the total cost of end user solutions which in turn will be dependent on the price charged by the service providers, and the extent to which the need for custom software can be minimized via the use of packaged software.

The speed users of CDPD can expect is a 1-5 second response time and raw data rate of 10.2kbps, and a sustained user throughput on the order of 9.6kbps. Security for CDPD is reasonable, since eavesdropping on the network is difficult.

The cost of CDPD is cheaper than switched cellular for the short messages typical of e-mail (less than 2-5 kb). Users are billed according to the amount of data transferred rather than by connection time or distance. Cost will probably be $.05 per kb, with 100 kb file costing close to $20 to transfer and a short e-mail around $.20.

Since the newer digital CDMA system can deliver data at 56kbps as opposed to CDPD's 19.2kbps, CDMA is seen by many in the industry as the logical successor, especially since security services in the CDPD protocol can reduce effective throughput to approximately 11-12kbps and since the CDMA frequency hopping protocol offers inherent security.

(Ref: http://www.raleigh.ibm.com.cel.celmel.html)

4.3.3.3 TDMA/CDMA/Steinbrecher Microcells:

The current Advanced Mobile Phone System (AMPS) cellular system is now yielding to the alternative TDMA and CDMA digital technologies. TDMA and CDMA are candidate technologies for the emerging Personal Communications Services (PCS) initiative. CDMA inherently offers greater room for improvement than TDMA does. While TDMA attempts to narrowly slice frequency bands, CDMA allows multiple frequencies to be used simultaneously. CDMA is inherently difficult to intercept since its 30 kHz cellular channel, is spread across a comparatively huge 12.5 MHz swath of the cellular spectrum. Many users share the same spectrum space at one time, since each phone is programmed with a specific pseudo-noise code, which is used to stretch a low-powered signal over a wide frequency band. The base station uses the same code in inverted form to "de-spread" and reconstitute the original signal. All other codes remain spread out, indistinguishable from background noise.

Both TDMA and CDMA technologies are equally applicable to the new PCS microcells, as well as to other types of wireless networks, but CDMA was the first to meet the tenfold call-carrying capacity increase that the industry originally called for. It can, in fact, provide up to a twenty-fold increase by assigning each call a unique code using up to 1/1000th of the required power compared to TDMA-based systems.

TDMA multiplexes up to three conversations over a 30 kHz transmission channel. It was seen as a quick start technology because it already had an established GSM market-base in Europe. As a result, TDMA was selected in 1989 as a digital cellular standard. Unfortunately, TDMA's three-fold increase in capacity has provided far less than the required ten-fold increase, and efforts are underway to increase its capacity.

CDMA technology, on the other hand, replaces frequency shuffling with digital intelligence. Supplanting the multiple radios of TDMA, where each connection exists on a fixed frequency, with digital-signal-processing that can find a particular message across a wide spectrum captured by one broadband radio. CDMA, in concert with the new Steinbrecher microcell appear to offer the potential to be technology leaders for the wireless industry. Rather than tuning into one fixed frequency, as current cellular radios do, Steinbrecher's microcells can use a high-dynamic-range digital radio to down-convert and digitize the entire cellular band. TDMA, CDMA, near or far, analog cellular, video, voice or data, in any combination, it makes no difference to the Steinbrecher system. Steinbrecher microcells convert them into a digital bit stream. Digital signal processors then sort out the TDMA and CDMA signals from the analog signals and reduce each to digital voice.

To the extent the Steinbrecher system prevails, it would end the need for hybrid phones and make possible a phased shift to personal communications network or a variety of other digital services. Steinbrecher radios could also facilitate the acceptance of CDMA. For CDMA, the microcell provides a new, far cheaper radio front end that is open to the diverse codes and fast-moving technologies of personal communications networks.

For the current cellular architecture, however, Steinbrecher microcells offers only creative destruction, doing for large base stations what the integrated circuit did for racks of vacuum tubes in old telephone switches.

The deployment of Steinbrecher microcells can significantly impact Coast Guard use of cellular service. The evolution of the cellular infrastructure from cells that require "high power" (600mw) link signal to the 6mw link microcell structure could impact the Coast Guard by reducing the effectiveness of cellular service in littoral areas where no microcells are available beyond coastal outlines.

The evolution to microcell technology may require the Coast Guard to deploy microcells aboard vessels, since the inter-cell links are not subject to the same low-power broadcast constraints as the hand-held phone to cell link. Also, the entire scope of this problem changes with the deployment of LEOS assets where potential to access space-based cells using a 0.7w signal from a hand-held cell phone will truly offer global connectivity. (C4I Technology Assessment, Pg. 39-40)

Several companies are currently deploying commercial CDMA service in the U.S. These include:

- AirTouch which introduced Powerband digital cellular service in Los Angeles. Powerband is the first large-scale commercial service offering in the U.S. based on

CDMA technology. Initial Powerband service in Los Angeles employs network infrastructure from Motorola and handsets from OKI and Qualcom Personal Electronics. The Powerband network will be comprised of more than 200 cell sites when the system is completed. Powerband has an average of nine times the call capacity of current analog systems.

- Bell Atlantic launched its commercial CDMA digital service in Trenton, New Jersey and Bucks County, Pennsylvania. Bell Atlantic NYNEX Mobile (BANM) reports a high level of customer satisfaction with the service. Currently, customers are paying $40 a month for unlimited calling in the 17 cell site area. Customers are particularly pleased with the superior voice quality. BANM's network provides eight to nine times the call capacity of existing analog networks. Furthermore, the system stability has exceeded expectations, with availability in excess of 99.8 percent. To take full advantage of CDMA's unique network characteristics, BANM employs a one-to-one analog to digital overlay in its cell sites. BANM engineers find that a one-to-one overlay allows for consistently better voice quality and considerably lower incidence of dropped calls.

- 360° Communications Company began offering CDMA service to its Las Vegas cellular customers. CDMA technology will enable 360° Communications to increase its network capacity to meet expected customer growth in Las Vegas, an area of extremely high cellular phone usage. The CDMA network has at least six times the call handling capacity of analog technology. Motorola provided the infrastructure and switching equipment for 360° Communications' entire network in Las Vegas. Qualcomm Personal Electronics furnished the dual-mode CDMA digital handsets for the service.

- GTE announced that it is conducting customer trials of CDMA technology in its Austin, Texas wireless market. The trials are intended to educate customers about CDMA technology and evaluate customer acceptance of voice quality and features, such as Caller ID and numeric paging. The customer acceptance testing follows operational reliability testing by GTE in the Austin market. Later this year, GTE will introduce a CDMA-based system in its San Jose, California market. Deployment in other major markets will commence in the near future.

4.3.3.4 Microcells

In cellular networks, any given area is segmented into cells with each having its own base station. The network design determines how many cells there are and how large an area they cover. Macrocells may have a range of 3 KM and a power of 6 Watts. Microcells are advertised with a range of .3 KM and a power of .6 Watt. The smallest of the cells are the picocells at a range of .06 KM and a power of .03 Watt. Other things being equal, smaller cell areas allow for higher traffic capacity. With smaller cell areas, the cost could rise since more base stations would have to be constructed and operated.

Current systems use macrocells, but future designs will use micro- and picocells. These microcell wireless access systems use fundamentally similar radio technology as compared to their bigger brothers the macrocells only with the reduced cell size (3 KM radius vs .3 KM radius). In the mobile environment the implication is that microcells have no inherent unit cost advantages over macrocells. Network operators should take care in making the switch from macro to micro only when capacity constraints require it.

Cell size implications in the maritime environment may mean a reduction in cellular coverage seaward if more systems convert to micro- or picocells. This should especially be true in metropolitan areas, where capacity requirements may force smaller cell sizes sooner. (Ref: http://www.wyoming.com)

4.3.3.5 CONDOR

CONDOR, offered by Qualcom Inc., is a secure, multi-mode hand-held cellular device that is capable of a broadcast mode. This system is designed to be used as a vital, secure communication system in Joint Services and covert activities. CONDOR may be poised to be extremely attractive to Coast Guard planners. A fully functional CONDOR, operating according to current designs, could provide the Coast Guard with an inexpensive automatic GPS locator system for emergency situations. A CONDOR unit can interoperate with:

- STU-III units;
- STU-IV units, also known as STE units;
- Cellular phone and pager service;
- FAX;
- E-mail; and
- Broadcast groups in a land mobile radio-like cellular broadcast arrangement.

In addition, the CONDOR unit offers features for:

- Local address book;
- Calendar;
- World time clock;
- Standard and predictive keyboards calculator;
- Paperless note pad;
- Appointment scheduler;
- Handwriting annotation; and
- Position locator that is accurate up to 100 meters.

These capabilities and features are available in a unit that is 2.5” wide, 1” deep, 8” long, and weighs only 18oz. The CONDOR unit can connect to local cells for local distribution or communicate world-wide via satellite when the Globalstar Low Earth Orbit Satellite (LEO) systems begin to deploy.

The CONDOR unit uses the FORTEZZA+ card to support STU-III interaction and to support secure Advanced Mobile Phone System (AMPS), Wideband Code CDMA, and Land Mobile Radio (LMR)-like communications.

The Federal Bureau of Investigation (FBI) has invested well over $10M in the development of this unit. They plan to make this the backbone of their various field units because of its versatility. It is felt that because of the support of this unit, by the FBI, and the importance of access to information in FBI files and data bases, **CONDOR will be recognized as the standard unit for law enforcement.**

The use of the CONDOR unit in the non-secure mode may be of considerable interest to the Coast Guard, since its use by the Coast Guard will interoperate with cellular phones readily available to the public, and thus reduce or eliminate mandates that the public buy specific safety equipment. The public may voluntarily migrate to cellular phone use out of self interest.

Table 4-9, below, (C4I Communications Technology Assessment pg. 42) shows how the flexibility of CONDOR prepares it to participate in a range of Coast Guard missions.

Table 4-9: CONDOR Mission Area Applicability

Mission Area	Condor Capability
Meet distress coordination, and command and control requirements in coastal areas and navigable waterways where commercial or recreational traffic exists.	The CONDOR system, with the advent of the Globalstar (LEOS) system, will provide world-wide coverage. The CONDOR is designed to automatically select cell or satellit readability.
Disseminate marine safety information.	The paging system or LMR broadcast modes could be use
Respond to crisis operations and provide sufficient voice channel and data communications capacity to support multiple operations.	The CONDOR system, using Spread Spectrum and CDMA make better utilization of the frequencies that have been allotted for the cellular phone system. This therefore provides for more users by a factor of 10.
Aid in searches for vessels that do not report, don't know, o incorrectly report their position, and assist in the prosecutio of hoaxes.	With the insertion of the GPS PCMCIA card in the CONDOR, it is possible to automatically relay location information to a Coast Guard station.
Record and time stamp voice re-transmissions and instantl play back incoming voice transmissions.	The CONDOR could incorporate voice mail with the pager function in the unit requesting that the caller enter their pho number for recall.
Allow communications with federal, state, and local government agencies.	If the cost of the CONDOR is in the price range of less tha $200, it will be used by many of the federal, state, and loca government agencies.
Protect the transmission of sensitive information.	The CONDOR system with the FORTEZZA+ card, will allo for encrypted data with protective keys to protect sensitive data.
Collect and disseminate intelligence and environmental monitoring/compliance data to/from mariners.	Using the CONDOR in the LMR mode will allow the Coast Guard to perform this function.

POC: Jim Treadway at Qualcomm Inc. (619) 658-2716)

There are several issues that represent a less desirable side of cellular phone use. Let's first look back to when Dick Tracy talked into his wrist. He had a little radio (and eventually, a tiny television) strapped there. The signal leapt, by the magic of comics, from Tracy's wrist to a satellite perched visibly over the buildings of the city like a Budweiser blimp. He could talk to anyone, from anywhere, because of that satellite. By now we are used to people flipping open cellular phones in restaurants, on ferries, in theaters, etc. But, Dick Tracy would have tossed today's cellular phones into a desk drawer and stuck with his wrist gizmo. Why? Today's cellular phones have ghosts and cross-talk. The spectrum is crowded. Other people can overhear—the underworld can certainly afford scanners. Sometimes when one "cell" hands you off to another, you get dropped like a trapeze artist with a timing problem. A cellular phone can't always call everywhere. A cellular phone can't easily leave town, and if you do, you pay extra to "roam."

4.3.4 Joint Maritime Communications Strategy (JMCOMS)

JMCOMS represents a revolution in Naval communications. It allows for a broad evaluation of the products and services needed to satisfy a multitude of evolving mission requirements. This approach leverages the latest advances in communications technology, commercial or military, and maximizes the utilization of communications assets and scarce bandwidth. JMCOMS is both a technical and program strategy that implements the communications portion of the Navy's Copernicus architecture for C4I. It will leverage COTS solutions and field user-pull, flexible, interoperable, multifunctional communications systems.

The JMCOMS Technical Strategy consists of three elements: the Automated Digital Network System (ADNS), the Digital Modular Radio (DMR) System (sometimes referred to as "Slice" Radio), and the Integrated Terminal Program (ITP).

- **Automated Digital Network System (ADNS):** The ADNS, which is the key to JMCOMS, will provide efficient networking and automation capabilities, and will ensure world-wide communications connectivity via radio frequency (RF) communications assets included in DMR and ITP. ADNS will leverage industry accepted standards for communications routing, switching, and management, and will employ COTS/GOTS hardware and software to provide timely, efficient, and seamless data delivery to and from all data users. ADNS networking capabilities will allow for the sharing of scarce communications bandwidth and will reduce reliance on "stovepipe" communications systems and dedicated bandwidth allocations. ADNS will effectively "pool" communications resources and remedy the problems caused by overloading or underutilization of communications circuits. Overall, ADNS maximizes information transfer efficiency and provides seamless afloat/ashore voice, video, and data networks for world-wide, interoperable communications.

- **Digital Modular Radio (DMR) System:** DMR will satisfy tactical communications requirements in the High Frequency (HF), Very High Frequency (VHF), and Ultra High Frequency (UHF) ranges. DMR will reduce the cost of acquiring and upgrading communications systems and will increase tactical flexibility. The DMR System will migrate from stand-alone, "stovepipe" terminal systems to a modular radio comprised of flexible, software configurable hardware modules. DMR will permit the on-scene-commander to reconfigure radio assets in accordance with changing mission needs. DMR will be compatible with ADNS for network control and monitoring capabilities. In addition, the DMR System will field integrated, multiband antennas that will reduce topside space and weight, and will lessen ship radar cross section. In short, DMR will provide affordable, flexible, interoperable, demand adaptive communications.

- **Integrated Terminal Program (ITP):** ITP will provide flexible and responsive subsystems and terminal equipment that will enable protected narrowband and wideband communications connectivity. ITP will satisfy communications requirements in the SHF, EHF, and commercial SATCOM frequency bands. This program will field a collection of military and commercial products that will evolve to further the JMCOMS objectives of providing increased communications connectivity and Joint interoperability. ITP will leverage commercial terminal systems and services, such as C- and Ku-band SATCOM, Direct Broadcast Satellite Service

(DBSS), INMARSAT, and GBS to support high data rate requirements for voice, data, imagery, and video (i.e., intelligence, weather, live video, news). ITP will place emphasis on COTS/GOTS components and will pursue "plug and play" modular terminal configurations. ITP capabilities, integrated with ADNS and DMR, will provide adaptable, Joint interoperable, protected, and high capacity communications at less cost.

(POC: http://www.spawar.navy.mil/pmw176)

4.3.5 Traditional Wireless Communications

With the advent of DoD Fleet Satellite Communications (FLTSATCOM), coupled with rapidly changing and improving satellite technology, SATCOM has become the primary carrier of global military communications. The existing HF network has assumed a secondary, albeit important, backup role in DoD. This is generally the case for larger Coast Guard cutters as well (i.e., 378s and 270s). However, the Coast Guard still relies heavily on HF as the primary means of passing record message traffic on smaller cutters (i.e., 210s and below).

It is now considered normal procedure for larger cutters (378 WHECs and 270 WMECs) to copy the Navy FLTSATCOM broadcast, while underway, and to also send their message traffic via Navy satellite circuits. Even the smaller 210 WMECs have satellite communications capabilities for copying the recently established Coast Guard Fleet Satellite Broadcast (LMCG). However, since the LMCG is a one-way, shore-to-ship broadcast system, the ship's outgoing message traffic is still sent via HF on-call radioteletype (RATT) circuits to a Coast Guard Communication Station (COMMSTA).

Smaller cutters (i.e., 110 WPBs) are not equipped to send or receive record message traffic via satellite. Therefore, their primary means of sending and receiving messages is the Coast Guard developed High Frequency Data Link (HFDL), a secure (KG-84), polled, packet-switched, wide-area data network that operates over HF radio..

The C4I Communications Technology document, developed by the C4I and Sensors Project Staff, indicates that several of the Coast Guard's primary mission areas have strong HF communications requirements. These mission areas include:

- Contingency Preparedness/Defense Operations (CP/DO;
- Enforcement of Laws and Treaties (ELT);
- Ice Operations and Marine Science Activities (IO/MSA;

- Search and Rescue (SAR); and
- Waterways Management and Aids to Navigation (WWM/ATON).

The primary HF communications requirements include the need for:

- Medium to high data rate Serial Tone Modems (STMs);
- Message processing systems interoperable with the Navy HF message delivery systems;
- Fast tuning, rapid frequency shift radios with ALE controllers;
- Secure voice and message communications;
- DSC installation;
- Improved equipment reliability and maintainability;
- Common crypto and crypto keylists; and
- Real-time data link for command and control of own units in local and multi-national operations.

The problem is that the most of these mission areas is now suffering from the lack of communications interoperability with the Navy. This is primarily due to the Navy's HF improvement process which has inserted new HF technology into the command and control systems, including HF Automatic Link Establishment (ALE), High Speed Fleet Broadcast (HSFB), and advanced HF radio systems with fast tuning capabilities (discussed later in this Section).

In addition, both the Navy and the Coast Guard have documented that certain cutters, particularly the 210' WMECs, do not have the communications capability to operate effectively together. Cutters and aircraft have requirements to communicate with their operational commanders. This requires rapid, secure communications which do not exist at this time.

Several new technologies can and will provide much needed improvements to the current HF system. Some of these new technologies are discussed below, based on information provided by the C4I Technology Assessment document dated 7 August 1996.

- **HF Transmitters:** Over the past several years, HF communications technology has made significant advances, and has again become a viable alternative for long-haul communications. New transmitter technology has replaced the large, slow, manually tuned transmitters of the past. These new transmitters are capable of fast tuning, with memory channels that permit rapid frequency shifts, and support other technologies, such as ALE. New transmitters can be controlled remotely using standard physical interfaces from either PCs or remote control units (i.e., COMMSTA Control System). The Coast Guard is currently replacing many of their old Rockwell HF80 transmitters with new Harris 750A 10kw transmitters, at a cost of approximately $77,000 each.

- **<u>HF Receivers:</u>** New HF receivers are solid state tuners with automatic digital controllers and pre-stored memory channels. These receivers typically have 100 channels of memory with pre-stored frequencies that permit rapid tuning. Tuning to new, non-prestored frequencies can be accomplished in fractions of seconds. Enhancements, such as digital signal processors (DSPs) have been introduced to increase accuracy and speed of received signal processing. The receivers are capable of multiple modes of operations, including the traditional Upper SideBand (USB), Lower SideBand (LSB), and Independent SideBand (ISB), and have built-in preselectors to reject strong signals from generating image signals.

- **<u>HF Transceivers:</u>** Old transceiver technology consisted of a transmitter or exciter and a receiver built into the same chassis with a transmit/receive switch to prevent receiver front-end selectors from being overloaded and destroyed. The transceiver components had the same characteristics as the individual components would have had if broken out into independent transmitters and receivers (i.e., slow, manual tuning, etc.). Old transceivers typically came with manually tuned couplers or remote couplers. New transceiver technology includes:

  - Auto-tuning;
  - Built-in preselectors to counter strong signals producing image frequencies;
  - Rapid tuning;
  - Built-in modems;
  - ALE; and
  - Memory channels for transmit and receive preset frequency storage.

  All transceivers are smaller than the generation they are replacing, and usually fit into a standard 19 inch rack. Some of the smaller units will fit on table tops, and are suitable for installation on small vessels. Transceivers are designed to operate in half-duplex or simplex modes of operations only, though it is within the means of the technology to build an offset receiver to provide full-duplex operations. Future technologies appear to be headed towards automatic control, greater efficiency and greater reliability.

- **<u>HF Modems:</u>** Older modems were independently setup and patched to supporting equipments, where record message traffic primarily used multi-tone modems. New modems support multiple modes of operations with greater power.

  The Navy has developed a new modem, the HF Data System (HFDS), which will be installed on high and medium endurance cutters, and on icebreakers. The HFDS can transfer data at speeds up to 2400 bps. Testing supports the expectation that 1200 bps could be expected under most circumstances, even with low power shipboard transmitters.

Another new modem technology is the ALE modem/controller. This modem is unique in that it controls multiple tasks associated with establishing connectivity automatically. This is done by sounding to determine the best frequencies available for a given service, performing link quality assessments on frequencies tested for connectivity between two points, and determining what platforms are able to communicate with the challenging or master station.

Future modem technologies appear to be headed for ALE networking vice point-to-point protocols, better automatic repeat request capabilities, and some exploration of spread spectrum waveforms.

ALE appears to work well in DoD, in a task group-type environment. However, was tested in the Coast Guard, a few years ago, and did not prove acceptable for Coast Guard multi-mission operations, especially where units may be required to communicate with the maritime public and other government, private, and public agencies.

- **HF Couplers:** The old couplers were slow, manually tuned multi-couplers, with some remote control capability. Some had motorized tuning capabilities, but none were digitally controlled and few had an automatic tuning capability to support transceivers. Older transmitter couplers are tuned by transmitting a signal through the coupler to the antenna and manually tuning until a peak or null indication is read on a dial, or by pushing a button until the coupler matches up impedance.

  New coupler systems are rapid tuning, digitally controlled couplers associated primarily with whip antenna systems. Some new technology couplers, that are adaptive and selective for both narrowband whips and broadband fan antennas, are emerging. These future couplers, which are still proprietary, seem to be evenly divided into two areas: multi-couplers for broadband antennas and narrowband couplers for whips and active antennas.

- **HF Antennas:** Little change has occurred in HF antenna technology in recent years. Some types of antennas have been removed from ships, and others, such as the loop antenna, have fallen from favor as transmitting elements. This was primarily due to their lack of omni-directional coverage, a requirement now considered important to mobile unit applications. The mainstays of antenna technology remains the narrowband whip and wire antennas, along with the broadband fan.

  Two new antenna technologies are just emerging and have not yet been tested. They include a whip antenna that has been optimized for use of higher frequencies for surfacewave paths, and a new broadband fan that is expected to have a more uniform impedance across the full HF operating spectrum.

- **HF Broadband Technology:** Broadband HF is a relatively new technology being introduced into major Navy command ships. The first broadband system in the Navy provided multiple HF circuit output to broadband antenna systems, and a broadband receive system to support multiple HF receive requirements. A limited number of narrowband components are included in the broadband system to handle Link-11. A newer broadband system has been designed by Harris based on the company's broadband system installed in Canadian frigates. The new system is more flexible than the old system, and comes in several configurations to match the platform's circuit requirements. Existing broadband systems are being backfitted with ALE capability. Future broadband technology appears to be looking at a means of reducing costs of current technology, and ways of integrating this technology into force operations, rather than developing a new broadband architecture.

- **HF Narrowband Technology:** Transmitter and receiver narrowband architectures are the most commonly used architectures used by the Navy and Coast Guard. These architectures provide advantages for:
  - Flexibility in design and upgrade;
  - Less expensive to procure;
  - Less expensive to install;
  - Only minor changes to the logistic system needed as new components replace older ones; and
  - Supports full-duplex operations.

  However, narrowband transmitter and receiver architecture is more difficult to automate due to the increased numbers of control lines required, and it may require more control software to be written to support different message format requirements. In addition, it does not support ALE from the perspective of requiring different antennas for the transmitter and the receiver, each with its unique radiation pattern, and it requires additional personnel staffing due to the patching requirements.

The Navy has issued a new HF policy designating HF as the media of choice for intra/interforce communications and for communicating with allied and coalition naval forces, as well as to support back-up ship-shore HF communications. One of the highest priorities in the National strategy, is to conduct all military operations as Joint operations, if only the U.S. is involved, or as combined operations, if allied or coalition forces are involved. In all cases, interoperability is the key word (discussed in greater detail in the next Section), and must be considered when selecting future voice, data, and video technologies. (C4I Interoperability Assessment Pg. 166)

Global Maritime Distress and Safety System (GMDSS)

The GMDSS is not a "system" in the conventional, communications sense, but rather an integrated approach for improving maritime safety and communications. This consolidated effort is planned to upgrade and enhance the following types of maritime operations:

- Alerting;
- Locating;
- On-scene SAR Communications;
- Meteorological, navigational, and urgent information;
- VHF-FM Bridge-to-Bridge communications; and
- General Business Communications.

The elements of the GMDSS, when implemented, will result in significant improvements in communications support for the above activities. All of these elements and the implementation requirements are defined by amendments to the 1988 Safety of Life at Sea (SOLAS). These agreements require certain types of communications systems/hardware to be installed on selected classes of vessels. The specific communications required are further defined by the ocean areas in which the vessel is operating. These operating areas are also defined in the agreements that implemented the GMDSS.

Several elements of GMDSS will have an impact on Coast Guard communications. The most significant of these elements are as follows:

- **Digital Selective Calling (DSC):** DSC is an alerting and radio circuit establishment feature that enables automatic initialization of communications between transmitters and receivers. (It is analogous to dialing a telephone number over the commercial telephone system.) Stations are notified of incoming traffic when their communications equipment receives the DSC data stream. DSC is envisioned for installation on Coast Guard Medium Frequency (MF), HF, and VHF (Channel 70) systems ashore and afloat. Prototype HF and VHF DSC systems have been installed at several Coast Guard locations for testing.

- **World-wide Navigational Warning Service (NAVTEX):** NAVTEX is the international standard for data transmission over MF, and has similar features and capabilities to Simplex Teletype Over Radio (SITOR), described below. Broadcasts, of urgent navigational, weather, and other warning information, are transmitted by Coast Guard COMMSTAs at scheduled times each day, in digital format, on 518kHz. It is essentially automated and runs on a Coast Guard Standard Workstation (CGSW). The Coast Guard currently provides this service to the maritime public and will continue to do so for the foreseeable future.

- **Simplex Teletype Over Radio (SITOR):** SITOR is the international maritime standard for transmission of data via HF radio. As the standard, it is used for the following:

  — All ship-shore, unclassified message traffic;

  — Non-voice distress communications; and

   — Communications with the civil maritime community, including NOAA and foreign military vessels.

  SITOR capability is already installed at the COMMSTAs and is planned for installation on WLB, WAGB, WHEC, and WMEC cutters.

- **INMARSAT:** Satellite communications capability is also required for commercial vessels under the GMDSS agreements. The vessel class and its ocean operating area determine which type of INMARSAT capability is required.

- **Impact of GMDSS on the Coast Guard:** International agreements require all SOLAS vessels to be capable of DSC operation on all of their radio communications not later than February 1999. The automatic nature of DSC operations will affect both radio operations procedures and personnel requirements. After February 1999, vessels meeting GMDSS DSC requirements are no longer required to guard Channel 16 VHF-FM. However, recreational boaters, and certain other maritime vessels, are not required under the SOLAS agreement to carry DSC. Therefore, the Coast Guard will still be required to maintain a VHF-FM distress guard on Channel 16 for non-DSC equipped vessels.

   — As elements of the GMDSS are implemented and integrated into the Coast Guard COMMSYS, voice communications over the System Coordination Network (SCN), 2182kHz, and VHF-FM Channel 16 may be phased out or discontinued.

4.3.6 Tactical Defense Message System (DMS)

As implementation of the Defense Message System (DMS) begins in earnest, at many shore commands, a question often asked is "What is the plan for ships?"

The Navy is committed to providing full DMS capability to ships and submarines. In many ways, the shipboard architecture may be similar to a shore command. However, since ships have more constrained and unique operating environments, the proposed implementation strategy and schedule will be different. Plans for tactical DMS have not been finalized.

The Navy plans to field Global Broadcast System (GBS) receive terminals on all classes of ships and submarines down to Coastal Patrol Craft. Within the next several years, however, the Navy will bring greater capability to more ships by fielding such programs as EHF Medium Data Rate terminals, more UHF/VHF radios and GBS terminals. DoD has also started fielding the Automated Digital Networking System (ADNS), which extends the NIPRNET (and its SECRET counterpart, the SIPRNET) to battlegroups and amphibious readiness groups.

It's expected that all surface ships will be able to receive the GBS by the year 2003. The goal is to have broadcast capability incorporated into the DMS components by FY99.

The NAVMACS system provides message processing and distribution aboard surface ships today. NAVMACS sends and receives messages in a variety of formats over different paths, such as Fleet Broadcast, CUDIXS. The NAVMACS systems are in the process of being replaced by NAVMACS II. NAVMACS II provides greater functionality at a cheaper cost using COTS equipment which users can access via existing shipboard LANs.

Since the NAVMACS II configuration of messaging file servers, with users connected to LANs, is very similar to the DMS philosophy, the Navy based its surface ship implementation strategy on evolving NAVMACS II to host DMS components.

For security purposes, each user will have a FORTEZZA card to access the DMS.

The NAVMACS II system, with DMS components, will provide flexibility in sending/receiving messages. As ADNS is fielded, and when bandwidth is available, NAVMACS II will receive messages in DMS format directly over the SIPRNET/NIPRNET backbone. Yet if needed, NAVMACS II will still be able to receive in the old formats (i.e., Fleet Broadcast, CUDIXS, etc.). The MultiFunction Interpreter (MFI), that will be included in NAVMACS II, will convert these old formats to DMS prior to sending them on to the user.

DMS messaging, aboard ship, will depend on a dedicated shore infrastructure. The NCTAMS currently provide the fleet gateways for AUTODIN messaging, and it is envisioned that they will continue in this role for DMS.

Technology for DMS, including bandwidth needed for surface ships, is here today.

To the shore user, the critical date is the closure of AUTODIN by December 1999. Through the use of an MFI, however, ships will be able to continue to receive message traffic in the current formats for as long as necessary. Eventually, ships will be able to send and receive DMS directly, all the time, to other DoD users. (POC: LCDR Bryant (703) 602-8361)

Figure 4-9 shows the proposed architecture for ship-shore DMS.

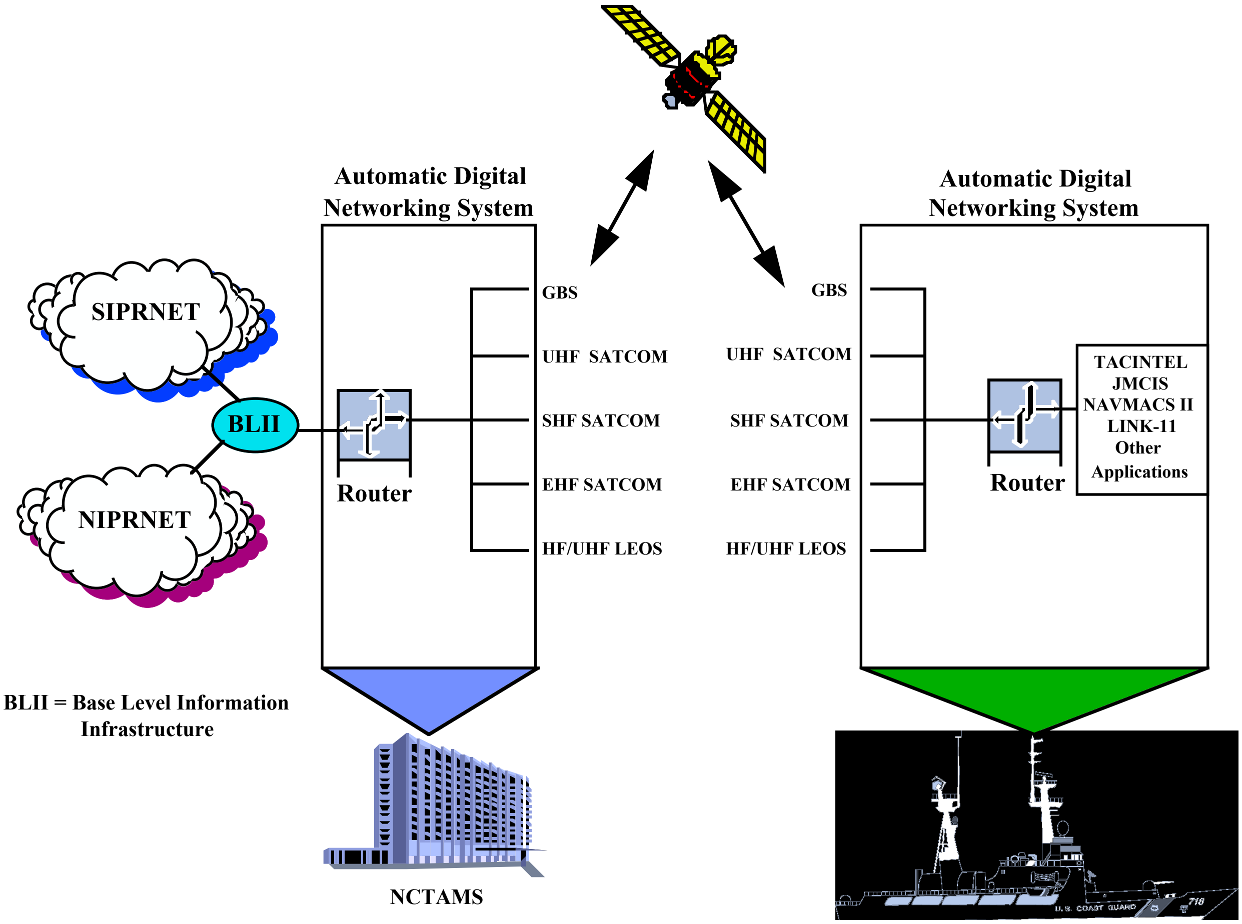


Figure 4-9: DMS Underway

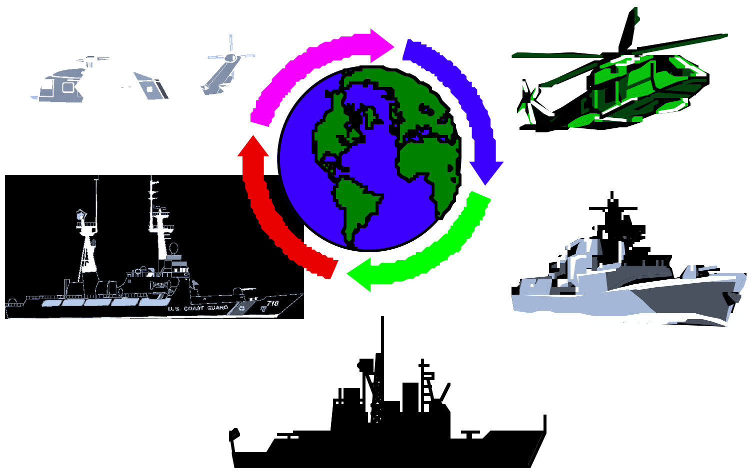
- **<u>DMS and the Coast Guard:</u>** Several classes of Coast Guard vessels have the ability to exchange organizational record messaging electronically. These range from 399ft Icebreakers down to 110ft Patrol Boats. The larger cutters (270ft and above) use NAVMACS or NAVMACS II as their messaging system. They send and receive messages via the Navy NCTAMS, which provides the interface to AUTODIN.

  The Coast Guard interface to AUTODIN is provided by one of 18 Message Distribution Terminal (MDT) sites. For vessels under 270 feet, messages are routed through Coast Guard Communication Stations (COMMSTAs). The COMMSTAs provide the shore-based interface to the CGDN and SDN for unclassified and GENSER classified messages, respectively. Messages are delivered via UHF SATCOM or HF, depending on the size of the vessel. Smaller ships typically use HF RATT or the polled HFDL

Specific plans for the implementation of DMS, in a tactical environment, have not yet been formulated. The Coast Guard is working with the Navy DMS Tactical Working Group to design this architecture. At a minimum, message format and protocol conversion will need to be provided by the implementation of an MFI at the COMMSTAs. The COMMSTAs will continue to provide the interface to the CGDN.

The Coast Guard is in the process of automating their tactical communications by installing a T-1 network between the COMMSTAs. By FY99, all COMMSTAs will be remoted to the two Communication Area Master Stations (CAMS).

4.4 DoD Interoperability



The Coast Guard operates in a multi-mission environment which includes increasing requirements to participate in combined operations with the Department of Defense (DoD). In a world of rapidly changing technology, the Coast Guard must be increasingly adaptable, flexible, and responsive to change. Coast Guard forces have taken this challenge to heart and are responding in a superb fashion. Streamlining efforts have produced a lean, efficient, and effective organization. One factor critical to continued mission success, improved readiness, and enhanced quality of life for mobile forces will be the ability to share information, seamlessly, and in real-time or near real-time through flexible, adaptable, interoperable communications systems.

The current communications systems will not meet the throughput demands of the future. Communication systems can no longer be developed, procured, and fielded to meet specific fleet operational requirements, and implemented in a "stovepipe" fashion. However, taking a "Network of Networks” approach will lead to the fielding of communications assets that are inter-operable and flexible enough to meet the throughput demands of today’s and tomorrow’s Coast Guard operational units. The future communication system must incorporate open systems architecture (OSA), and "plug and play" modularity to be easily reconfigurable and upgradable.

This Section of the TCP explores several technologies that are applicable to Coast Guard communications interoperability with the Department of Defense. For the purpose of this Section of the TCP, these technologies have been analyzed at a high level to determine their potential for addressing current and future requirements, and their impacts on the Coast Guard’s future telecommunications architecture.

4.4.1 Technologies

A combination of several current and emerging telecommunications technologies, each with unique capabilities, will be used in conjunction with one another to make up the future "Network of Networks". This all encompassing system will move all types of information seamlessly from place to place within the Coast Guard and also interface with other government agencies through direct circuits and network gateways. Some of these technologies are already in place and in operation, some will be the result of future procurements, and others will be provided to the Coast Guard by DoD to promote interoperability, and support the requirement for Coast Guard/Navy compatibility.

The "network" will provide several basic services. These include record message traffic delivery, electronic mail, and providing the transport medium for mission essential applications.

4.4.1.1 Dedicated Department of Defense Networks

Until security services to support the transport of sensitive information over commercial carrier services becomes viable, dedicated networks will continue to be important resources. The evolution of the Defense Data Network into the Defense Information System Network (DISN) and the Integrated Tactical/Strategic Data Network into a worldwide information transfer infrastructure supporting National Defense Command, Control, Communications, Computers, and Intelligence (C4I) requirements as well as Corporate Information Management and Defense Information System areas is well underway. The DISN focuses on providing integration of current systems, encompassing the period through the mid-1990s, and providing long-haul transmission services as well as a data transport service. The DISN includes point-to-point transmission, switched data services, video teleconferencing, etc. (C4I Interoperability Assessment Pg. 17)

The Coast Guard will directly interface with the DISN to obtain DoD long-haul data transmission services, and to maintain required compatibility with the Navy. This will be accomplished in conjunction with the planned implementation of the Defense Message System (DMS), which replaces the current world-wide Automatic Digital Network (AUTODIN). Interface (or gateway) locations have not yet been determined.

4.4.1.2 Defense Message System (DMS)

DMS provides secure, accountable and reliable messaging services, fully integrated with a global DoD directory service, based on Joint Staff validated requirements. It has a robust set of services that will work writer-to-reader, desktop-to-desktop within DoD and externally. With these capabilities, you will be able to access global directories from anywhere in the world, complete with addressing, security, and user capabilities information for all of the messages you compose and receive at your desktop.

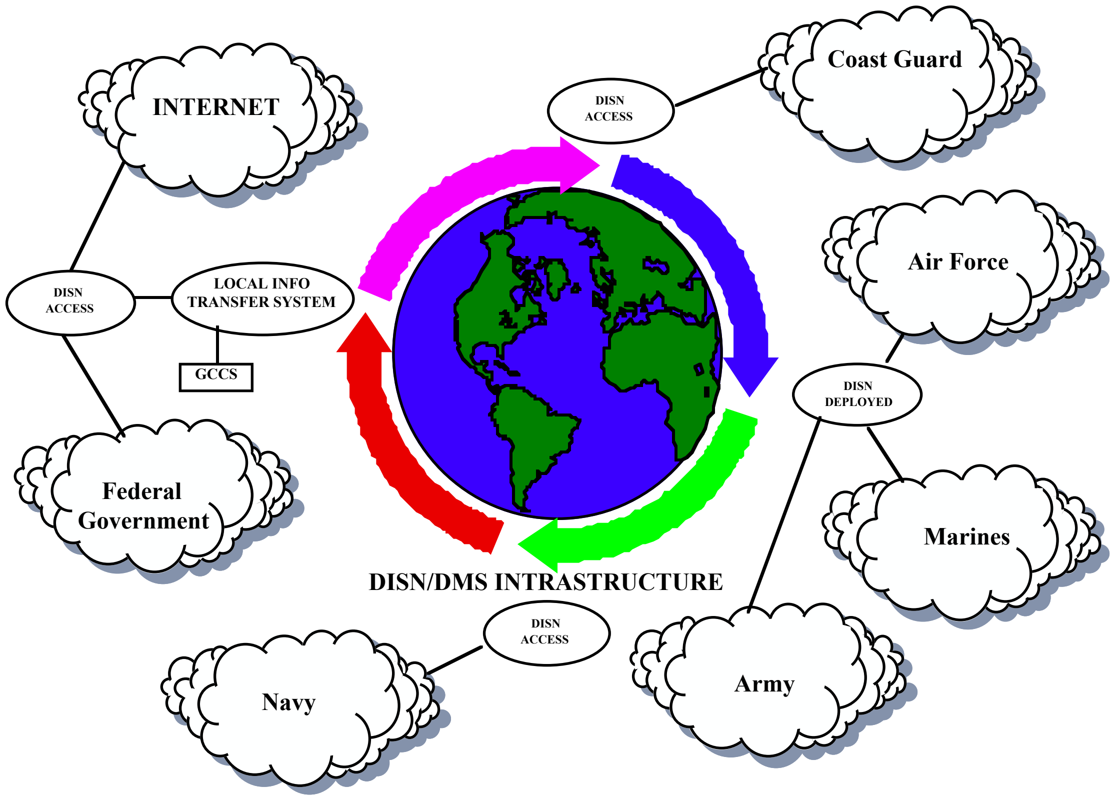


Figure 4-10: Defense Message System (DMS)

DMS will be implemented with commercial-off-the-shelf (COTS) products to be based on a set of international, open-system standards that provide full interoperability from writer-to-reader.

Additionally, DMS will provide interfaces to and interoperability with other federal agencies, our Allies, the commercial sector and the public. This is being done using a standards-based suite of products that ensure writer-to-reader messaging services and global directory capabilities, without the use of gateways.

The following DMS training courses are available through DISA's contract with LORAL Federal Systems. They are designed to be taught at either a Government facility or by the contractor, for individual users or for/by Government Instructors:

- Basic User Training Course
- Operating System Administrator (OSA) Course
- Message Handling System (MHS) System Administrator Course
- Directory System Administrator (DSA) Course
- Management Workstation Product (MWS) Course

Users can also order any of the above training courses from commercial vendors off the DMS contract. The Basic User Training Course can be taught to a maximum of 25 students per class.

All other training courses are taught to a maximum of 10 students per class. The number of DMS gateways will directly affect the amount of DMS training that is required.

Costs and architecture for Coast Guard-wide DMS implementation are not yet fully developed. However, the Coast Guard is well positioned to effectively integrate DMS and its desktop-to-desktop capabilities building upon the foundation of the Coast Guard Standard Workstation III transition currently in progress.

(Ref: http://www.spawar.navy.mil/pmw-176)

A government-wide e-mail Program Management Office (PMO) has been established within the General Services Administration (GSA) to support the development of service that appears to the user to be a single, unified electronic postal system. This system will offer robust and trustworthy capabilities with legally-sufficient controls for moving all forms of electronic information among employees at all levels of government, and with the public.

Like the nation's telephone network, government-wide e-mail needs to be affordable, efficient, accessible, easy-to-use, reliable, cost-effective, and supported by an effective directory service. The DMS program is being designed to support the exchange of e-mail with the government-wide e-mail system, and will allow an interchange of e-mail between DMS and commercial/other government agency (OGA) domains.

The DMS program is described in the "U.S. Coast Guard Information Security" document in the section entitled "FORTEZZA and DMS." Both programs will share many features and structures in common, but e-mail exchange within the DoD DMS community may be segregated.

There are many considerations to adoption of an e-mail strategy, including infrastructure requirements, interoperability limitations, translation gateways, maintenance of records, user accountability, firewall configuration, public access, organizational release requirements and procedures, use in the tactical environment, and many others.

The DMS program is implementing multi-function interpreters (MFIs), that provide protocol translation for interoperability with legacy systems during the transition and with non-DMS compliant systems external to the DoD after achievement of the objective DMS system.

The specifications for DMS do not clearly describe how DMS users can communicate with external or legacy users who are not provided with FORTEZZA cards.

No formal training, on this technology, is being offered at this time.

(Ref: C4I Interoperability Assessment, Pg. 18-19)

4.4.1.3 Military Satellite Communications (MILSATCOM)

Coast Guard assets have no cost access to certain MILSATCOM systems based on unique operational requirements and interoperability needs with the U.S. Navy. The Navy UHF Fleet

Satellite Communications (FLTSATCOM) system consists of leased and Navy owned satellites that provide world-wide communications connectivity with naval ships and airborne platforms. The FLTSATCOM system comprises space, earth, and control segments. Space and earth segments consist of satellites, earth terminals, subscribers, and subsystems. FLTSATCOM subsystems most commonly used by Coast Guard units are:

- Officer-in-Tactical Command Information Exchange Sub-system (OTCIXS) which provides a two-way link to support inter- and intra-battle group over-the-horizon targeting tactical command and control data communications in a near-real-time (1-15 minutes) environment. It provides a gateway to the SIPRNET which allows bi-directional tactical data links between shore commands and OTCIXS equipped units. OTCIXS is currently used by 378s and 270s, and is being installed on 210s and Transportable Communications Centrals (TCCs).

- Common User Digital Information Exchange Subsystem (CUDIXS)/Naval Modular Automated Communications Sub-system (NAVMACS) provides a 2400 baud full duplex interface over a satellite link with mobile platforms. NAVMACS provides up to four channels of fleet broadcast input, a subscriber interface to CUDIXS and other on-line message functionality. NAVMACS on Coast Guard cutters is configured with Coast Guard Standard Workstation (CGSW) equipment and supported by the Shipboard Telecommunications Computer System (STCS).

- UHF Demand Assign Multi-Access (DAMA) Sub-system provides users with increased communications capacity and reliability over dedicated access on the FLTSATCOM satellites. DAMA is capable of multiplexing secure voice, record message, and data sub-systems onto a single 24 kHz satellite channel. WAGBs, WHECs, and 270s have DAMA, while 210s and the TCCs are being upgraded.

Military Strategic, Tactical, and Relay (MILSTAR) is a military satellite communication (MILSATCOM) system that provides highly robust, secure, and survivable communications among fixed-site, mobile, and portable terminals. Operating primarily in the extremely high frequency (EHF) and super high frequency (SHF) bands, MILSTAR satisfies the US military's hard-core communications requirements with worldwide, antijam, low probability of intercept (LPI), and low probability of detection (LDP) communications services.

In the MILSTAR EHF and SHF bands, small antenna apertures produce narrow beams, which are difficult to jam, with high transmit and receive gain.

The MILSTAR payloads perform extensive on-board processing of the uplink and downlink waveforms for efficient on-orbit resource use and maximum antijam performance. On-board signal processing ensures full interoperability among the military services and other users who operate terminals on land, sea, and in the air.

Often described as a switchboard in the sky, the MILSTAR payloads have on-board computers that perform communications resource control. MILSTAR responds directly to service requests from user terminals without satellite operator intervention, providing point-to-point communications and network services on a priority basis.

The MILSTAR payloads can reconfigure in real-time as users' connectivity needs change, providing the dynamic communication networks that highly mobile tactical warfighters require.

Worldwide connectivity is established using space-to-space satellite crosslinks. Crosslinking allows user communication networks to extend around the globe without retransmission, through intermediate ground stations. Crosslinking also provides worldwide command and telemetry access to every MILSTAR satellite.

The entire MILSTAR constellation can be operated through the crosslinks from a single CONUS-based mission control station; potentially vulnerable foreign control sites are not required.

Each MILSTAR satellite has a mass of approximately 10,000 pounds and produces nearly 5000 Watts of solar array power. The first two MILSTAR satellites (called MILSTAR I) have a low data rate (LDR) payload. The third and subsequent vehicles (MILSTAR II) feature a medium data rate (MDR) payload. The completed MILSTAR II constellation will consist of four satellites in near-geostationary equatorial orbits.

- **MILSTAR Highlights**:
  - Global coverage via Earth coverage, agile, and steerable antennas;
  - Automatic terminal logon and network setup procedures;
  - Assured global connectivity via onboard router, processor, and crosslinks;
  - CINC-controlled resource allocation for dynamically changing situations;
  - Flexible communication services:
    - Point-to-point
    - Conference network
    - Broadcast
    - Voice, data, imagery, and video teleconferencing capabilities;
  - Throughput rates to simultaneously support Navy battlegroups, shore stations, and Naval independent operators;
  - LPI/LPD to protect terminal assets and special operations;
  - UHF capability and EHF/UHF crossbanding for interconnecting with AFSATCOM and fleet broadcast terminals;
  - Interoperable waveforms and data rates;
  - Robust, antijam, waveforms;

- Nulling antennas for in-beam jamming protection; and
- Communications Security (COMSEC)/Transmission Security (TRANSEC) protection with over-the-air rekey (OTAR) capability/specifications.

No significant increase in current training requirements is expected.

(POC: Steve Johnson at msl@leonardo.jpl.nasa.gov)

4.4.1.4 Electronic Data Interchange

Electronic Data Interchange (EDI) efforts are intended to extend the benefit of information systems applications to transactions conducted between autonomous activities. Information and communications technology that is needed to build inter-organizational systems has been available since the late 1960s. However, the relatively slow adoption of inter-organizational systems suggests that they have to be viewed not primarily as technically-driven, but rather as business-driven systems. Early examples are computer-reservation systems in the airline industry, inter-bank systems for funds transfers, and ordering systems in the auto industry. They underscore the purpose of inter-organizational systems which is to facilitate official transactions among cooperating activities.

Inter-organizational transactions improve the speed, ease, and quality of information transfer, and extend the concepts and goals of office automation into the inter-organizational realm. EDI is the inter-organizational, electronic exchange of standardized messages among applications. *EDI enables organizations to exchange any structured document in a standard format among their applications with little or no human intervention*.

A crucial part of EDI is the message standard. Standardized messages are the precondition for an automated exchange and interpretation of the message contents. In order to facilitate international trade and commerce, the United Nations has taken over the responsibility to develop a message standard for EDI known as Electronic Data Interchange for Administration, Commerce, and Transport (EDIFACT).

Although the development of a global business language (i.e., message syntax that can be used independent of hardware and software, is a long and tedious process, the advantages over bilateral, sectoral or national standards are considerable. The goal of the implementation of EDI based on EDIFACT is to conduct entire business transactions with multiple partners, such as suppliers, customers, service providers, peer agencies, banks, etc., based on a single technology and a single standard.

According to the philosophy of the ISO/Open System Interconnection (ISO/OSI) model of communication that distinguishes different functional layers and in order to avoid unnecessary rigidities, EDIFACT covers only the message syntax. How the messages are actually transferred among the partners depends on the communication technology that is available and on their needs in terms of bandwidth, security, and level of service. E-mail exchange standards, such as INTERNET's Simple Message Transport Protocol (SMTP) and CCITT X.400 are ideal candidates for a low cost transmission of EDIFACT messages. Other standards and telecommunication services are available and are offered by the National Post, Telephone, and Telegraph (PTT) or private Value-Added Network (VAN) service providers.

Like many other technologies, EDI has been accepted more slowly than expected. EDI has been perceived as too complicated, activities did not know how to integrate EDI into their applications, standard messages were not available, and the number of potential partners was relatively low. However, this situation has changed significantly. Throughout the world, the number of activities that use EDI has risen. Large companies demand that their business partners be able to accept EDI messages (and in many cases assist them in setting-up the requisite technology). Public sector initiatives, like the Clinton administration's Electronic Commerce for Acquisition initiative will accelerate acceptance of EDI.

Three perspectives can be distinguished for electronic commerce on the INTERNET and EDI:

- The INTERNET can be used to transmit EDI messages;
- Standards for the inclusion of EDIFACT messages as bodies of e-mails sent via the INTERNET have been developed. Transmission costs are significantly lower than traditional communication via PTTs or VANs, but reliability and security are a concern of many potential users;
- EDI application can be built upon the World Wide Web (WWW) providing an easy to use interface for the customer, and generating EDIFACT messages (e.g., orders or payment orders) transparently. The advantage of this solution, is that the EDIFACT application actually (because of the underlying client-server architecture) resides at the provider's system, the customer only needs a WWW browser and INTERNET access.

EDI and WWW services can be seen as complimentary: while EDI focuses on standardized business transactions, WWW applications focus on the transmission of multimedia information.

No significant increase in current training requirements is expected.

(Ref: C4I Interoperability Assessment Pg. 21-24)

4.4.1.5 Defense Satellite Communications System (DSCS)

The Defense Satellite Communications Systems (DSCS) is an important part of the comprehensive plan to support interoperability of globally distributed military users.

Currently, two Phase II and eight Phase III DSCS satellites orbit the earth at an altitude of more than 23,000 miles. DSCS III also carries a single channel transponder used for disseminating emergency action and force direction messages to nuclear capable forces. Each satellite utilizes six super high frequency transponder channels capable of providing worldwide secure voice and high rate data communications.

The system is used for high priority communication, such as the exchange of wartime information between defense officials and battlefield commanders. The military also uses DSCS to transmit space operations and early warning data to various systems and users.

The first of the operational DSCS II satellites was launched in 1971. Their two-dish antennas

concentrate electronic beams on small areas of the Earth's surface, but have limited adaptability in comparison to the newer DSCS III.

The Air Force began launching the more advanced DSCS IIIs in 1982. The system is built with single, multiple-beam antennas that provide more flexible coverage than its predecessors. The single steerable dish antenna provides an increased power spot beam which can be tailored to suit the needs of different size user terminals. DSCS III satellites can resist jamming and are expected to operate twice as long as DSCS IIs.

DSCS users operate on the ground, at sea, or in the air. A special-purpose (AFSATCOM) single channel transponder is also on board the DSCS III satellite. Members of Air Force Space Command units, the 50th Space Wing's 3rd Space Operations Squadron at Falcon Air Force Base, Colo., and 5th Space Operations Squadron at Onizuka Air Force Station, Calif., provide command and control for all DSCS systems.

(Ref: http://www.laafb.af.mil./smc/mc/dscs.html)

(Ref: http://www.disa.mil/org/disad321.html)

4.4.1.6 Global Broadcast System (GBS)

The GBS will "push" a high volume of intelligence, weather, and other information to widely dispersed, low cost receive terminals, similar to the commercial DBS. The system will include a capability for users to request or "pull" specific pieces of information. These requests will be processed by an information management center where each will be prioritized, the desired information requested, and then scheduled for transmission.

Acting in response to a request from the Space and Naval Warfare Systems Command, NRaD has submitted a proposal for an X-band Global Broadcast Service (GBS) demonstration system. This system would use DSCS to demonstrate a way to provide GBS service to the military using government owned space assets and current terminal hardware. The plan is to demonstrate the utility of such a system by moving some of the current UHF and SHF traffic onto the X-band GBS broadcast. This would fit into the proposed GBS concept by providing the “intelligent push” type data, and also fits the requirements stated in the GBS Mission Needs Statement. The X-band system would provide a limited data rate Navy Broadcast capability. It would require modified SHF terminal hardware.

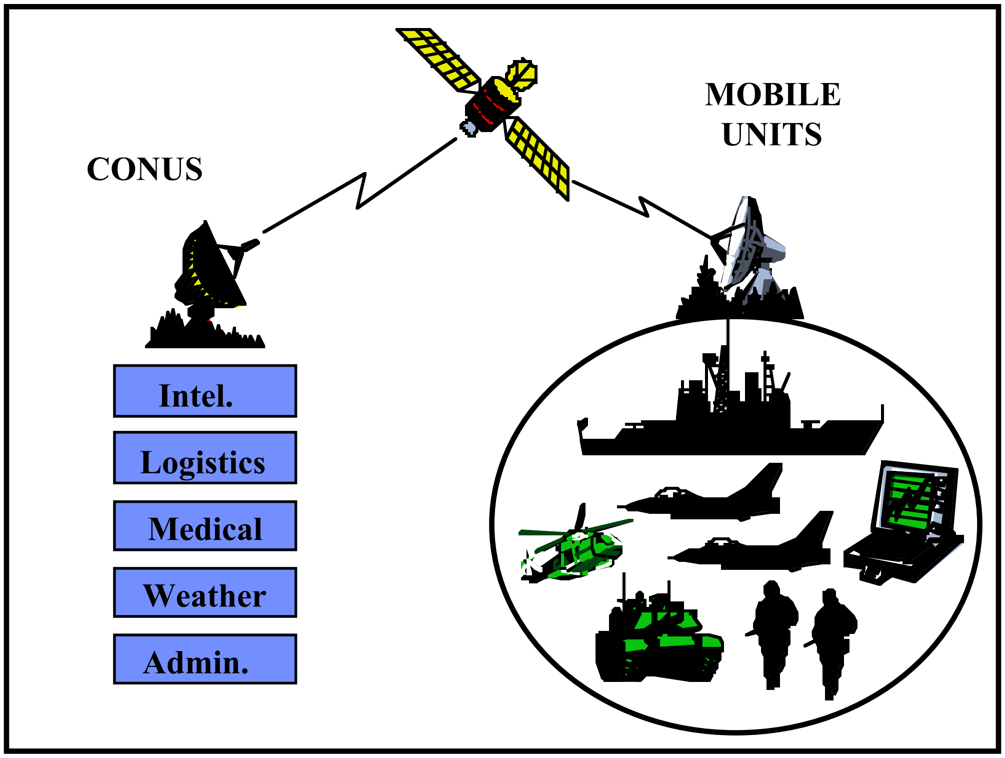


Figure 4-11: Interoperable Global Broadcast System

The concept is to put a GBS link on the DSCS immediately. This would provide a system to develop and test a concept of operations. It would provide a way to test network protocols and determine which services should be provided. The net would be moved to the GBS when the full satellite system is fielded. The current Army, Air Force, Marine Corp., and Navy SHF terminals would be used. The broadcast would be truly Joint.

In 1994, the Navy and Marine Corp. conducted a Joint Warfare Interoperability Demonstration (JWID-94). That demonstration was followed by JWID-95. There are significant differences between JWID-95 and other military exercises. The understood purpose of JWID-95 is to push the state-of-the-art. In exercises there is less impetus to try new and innovative concepts because there is pressure to ensure that everything works as planned. In JWID-94, there were mostly standalone demonstrations. In JWID-95, there was an increasing emphasis to integrate the C4I demonstrations to enhance total system performance. The objective is not to automate existing systems, but to develop new approaches to improve C4I for the warrior. As such, JWID-95 was an excellent opportunity to show the military operators the capability that this system can bring to the warfighter. The GBS demonstration that was done during JWID-95 transmitted data over the commercial DBS satellite at the 23Mbps data rate. Several types of data, mostly tactical intelligence, were successfully transmitted.

Hughes builds the UHF Follow-On (UFO) satellites, which share a lot of the common spacecraft bus hardware with the DBS satellites. The intent is to modify Flights 8, 9, and 10 of the UFO program to include the high power wideband transponder for the GBS application. The first of these is scheduled to fly late 97 or early 98. The operational concept is to have some bandwidth set aside for general broadcast (producer-push) similar to Tactical Related Applications Broadcast and Fleet Broadcast (the first two world-wide broadcast systems) and some for query services (user-pull) response. The actual data format is being defined as is the frequency of the broadcast with SHF (X-band) favored over the Ka-band (20gHz). The JWID-95 data format was ATM and straight digital video in the commercial DBS format.

The GBS user hardware suite includes a 1 meter dish, a commercial receiver, a rate buffer module that provides the data interface to a user's computer equipment, and a HG-194 cryptographic unit. The cost for this hardware suite is roughly $40,000.

(Ref: C4I Interoperability Assessment Pg. 101-102)

4.4.1.7 Cellular Telephone

Communication across Circuit-Switched Cellular Networks involves the use of a cellular phone for voice communications or attaching a wireless computer modem to a cellular phone for data communications. Connection via an air-link through a nearby cell, then through the regional switch and ultimately through the telephone network to another computer is continuous until the link terminates when one participant hangs up.

The existing analog cellular network has a huge installed infrastructure providing "seamless" (since 1992) coverage, but only moderate speed (slower than spread-spectrum technology or Cellular Digital Packet Data (CDPD)) and high cost (more expensive, for example, than spread-spectrum or satellite transmission). Transmission of data is billed by the minute rather than by the character or kilobyte, in some cases yielding up to ten times the price of other wireless services to transmit identical quantities of data. The service offers access to the information services, like INTERNET, America Online, and CompuServe.

For 35 years, the wireless communications industry has been inching up the spectrum, shifting slowly from long and strong wavelengths toward wide and weak bands of shorter wavelengths. Transportable phone services have moved from the 1950s radio systems, using low FM frequencies near 100MHz, to the 1960s spectrum band of 450MHz, to the current cellular band of 900MHz, accommodating more than 23 million cellular subscribers in the U.S. During the 1990s, this trend will accelerate sharply. Accommodating hundreds of millions of users around the world, cellular communications will turn digital, leap up the spectrum, and may even move into video.

As stated in Section 4.2 (Mobile Communications), the CONDOR product from Qualcomm Inc. will have a potential impact on the Coast Guard. CONDOR is a secure, multi-mode hand-held cellular device that supports Code Division Multiple Access (CDMA) when available, and Advanced Mobile Phone Service (AMPS) and Time Division Multiple Access (TDMA) when CDMA service is not available. The CONDOR is also capable of a broadcast mode that can serve in place of land mobile radio (LMR) capability.

The Federal Bureau of Investigation (FBI), the Drug Enforcement Agency (DEA), and Joint Chiefs of Staff are very interested in CONDOR, and together with the National Security Agency (NSA) are making a significant investment in secure CDMA technology.

The CONDOR units use the FORTEZZA-plus card to support STU-III interaction. Future versions of the FORTEZZA-plus card (known as the FACET encryption card), due to be released in late 1997, is planned to be integrated into the CONDOR product. The FACET card will allow for Type-1 encryption over networks. This same standard adapter on the CONDOR unit supports any of several GPS adapters. The Federal government (in a variety of agencies) is expected to buy up to 1.4 million CONDOR units. Of these units, 350-450 thousand are expected to be Data Encryption Standard (DES) protected and 10-15 thousand Type-1 protected. It is also expected that state and local governments will purchase 4-5 million units.

This system is designed to be used as a vital, secure communication system in Joint Services and covert activities. CONDOR may be poised to be extremely attractive to Coast Guard planners. A fully functional CONDOR, operating according to current designs, could provide the Coast Guard with an inexpensive automatic position location capability, with an accuracy of 100 meters, using Globalstar, for emergency situations. This may provide the Coast Guard with DoD and OGA interoperability in support of Search and Rescue, Law Enforcement, and disaster response operations. The estimated cost for the instrument is targeted for $100-125 each.

Cellular technology may provide a high level of interoperability between the Coast Guard and DoD for both voice and data communications. Cellular telephone capabilities may be especially useful for communicating across agency boundaries during emergency or disaster operations (i.e., natural disaster, hurricane, flood, etc.), and simulated and actual wartime operations.

(Ref: C4I Technology Assessment, Pg. 40-41)

4.4.1.8 American Mobile Satellite Corporation (AMSC)

The first U. S. based mobile satellite service provider was American Mobile Satellite Corporation (AMSC). They currently have one satellite in orbit and authorization for two more. The operational unit has 2000 6kHz voice grade channels. AMSC's partner, Telesat Mobile Inc. of Canada was due to launch an identical satellite in early 1996. With that addition, the two companies will provide redundancy for each other in the space segment of their systems.

The AMSC mobile digital telephone service is called "Skycell Satellite Roaming Service" or "Skycell". Customers will access Skycell through dual mode satellite/cellular telephones that will be offered by two commercial vendors. These mobile telephones will first seek an available cellular system. In the absence of cellular coverage, the call will be automatically processed over AMSC's satellite system. In this case, the signal will be sent up to the satellite, then down through one of AMSC's primary gateway hubs. The hub will process the call and connect it to the long distance network which will deliver it to the local public switched telephone network (PSTN). The local network will then forward the call on to it's destination. Skycell service complements the current terrestrial cellular system in the U.S. Skycell features include:

- Directory Assistance;
- Operator Assistance;
- One Touch 911;
- Call Forwarding;
- Call Waiting;
- Three Party Calling;
- Conference Calling;
- No Answer Transfer;
- Call Restriction; and
- Voice Mail.

In addition to the dual mode satellite/cellular telephone service, AMSC will introduce a series of satellite only mobile telephone products to serve a variety of market needs. Included in this market is corporate and general aviation, private and commercial ships, and *law enforcement agencies*. This product serves those customers who need telephone communications wherever they go.

AMSC has stated that they will lease satellite channels (power and bandwidth) to the U.S. Government for use in private networks on a yearly basis. They have stated that they are willing to negotiate the number of channels as well as the length of lease. Prices will be negotiated based on lease period, but a price of $200,000 per year for one 6kHz channel was quoted in early October 1995. The same terminal equipment will be used on leased channels as with the Skycell option.

- **Terminal Equipment:** Terminal equipment will be available in the form of small, lightweight, mobile satellite/cellular systems and the satellite-only mobile telephone systems. Additionally, fixed sight terminals will be available. Available terminal equipment provides voice, secure voice (using STU-III), facsimile, and a full duplex personal computer data port using Hayes V-24 modem commands. These services are available at data rates of 2.4kbps and 4.8kbps. Prices for this service (Skycell) are projected to be $1.49 per minute with a $25.00 per month access fee.

AMSC's satellite/cellular telephone service looks to be an attractive addition to the telephone services now available from cellular providers, and this is evidenced by the extensive Government involvement with AMSC. It is also an attractive alternative to the more costly INMARSAT system for cases where the user stays within the AMSC satellite footprint. AMSC satellite spot beams cover all of the continental U.S. and Canada with coverage out to 200 miles offshore, Hawaii, and the entire Caribbean area. Both terminal cost and the per minute and monthly access fees are less expensive than INMARSAT.

AMSC provides similar capability to INMARSAT, but with a maximum data rate of 4.8kbps. One drawback is that both AMSC and INMARSAT equipment would need to be retained/maintained because they are incompatible systems. Both of these systems have a potential to meet DoD interoperability requirements by providing a common, reliable, rapid, and secure system for inter-agency voice and data communications.

(Ref: C4I Interoperability Assessment Pg. 92-95)

4.4.1.9 International Maritime Satellite (INMARSAT)

INMARSAT offers the following service types:

- INMARSAT-A: Supports high-quality direct-dial telephone, telex, facsimile, and data services;

- INMARSAT-B: Provides a similar range of services to INMARSAT-A, but, because it is based on modern digital telecommunications technologies, INMARSAT-B terminals are smaller, lighter, and cheaper to buy and incur lower user charges;

- INMARSAT-M: Terminals are the size of a briefcase. Provides direct-dial telephone, facsimile or 2.4kbps data connections. Maritime versions are fitted with tracking antennas with radomes about one eighth the volume of their bigger, more capable INMARSAT-A/B brothers. Terminal and user charges are also considerably less than those for the larger systems;

- INMARSAT-C: Lightweight, compact, and comes with omni-directional antenna systems. The terminals come in fixed, mobile, transportable, maritime, and aeronautical versions. INMARSAT-C supports two-way, store-and-forward message, text, or data reporting communications at a data rate of 600bps. INMARSAT-C supports two-way global messaging, fax, and e-mail. Services include: position and data reporting, weather forecasts, and electronic chart corrections; and

- INMARSAT-Aero: Provides store-and-forward text or data messages; real-time, data-only communications; and multiple-channel, flight-deck voice telephony.

INMARSAT is developing a revolutionary system called INMARSAT-P, which will facilitate the development of a global handheld satellite phone system, and allow direct satellite access from the one portable phone anywhere in the world. Current satellite telecommunications systems use geostationary satellites circling the earth 25,000 miles above the equator, once every 24 hours, the same as the earth's own orbit. INMARSAT-P will use a system of ten satellites which will orbit the earth once every 6 hours at a height of about 6,210 miles. Because these satellites are angled from the equator, telephoning will be possible from remote areas, such as the North and South Polar regions. The portable phone will be connected to the nearest satellite connecting station via satellite. The call is then connected to existing public networks and the receiving party's phone.

The range of products and services which will be supported by the INMARSAT-P system include a dual-mode cellular/satellite handheld phone supported by network integration with cellular systems. This will enable a caller to access terrestrial cellular links, when they are available, and satellite links, when terrestrial links are not available. Twelve access nodes will form a network to link INMARSAT-P satellite phone callers to public terrestrial and cellular networks. Based on the expenditures and backing to date, INMARSAT-P will be a major player in the LEOS market. (Ref: C4I Interoperability Assessment Pg. 116-118)

Table 4-10: INMARSAT-P Satellite System Information

Service Types:	Voice, Data, Facsimile, Paging
Data Rates:	4.8kbps voice, 2.4kbps data
Voice Circuits per Satellite:	4500
System Cost:	$2.6B(U.S.)
User Terminal Cost:	approximately $1000
Dual Mode User Terminal:	Yes (regular cellular and satellite)
Handheld User Terminal:	Yes
Operational Startup:	the year 2000
Satellite Lifetime:	10 years
Call Charge Rates:	$1-$2 per minute

Ref: http://www.worldserver.pipex.com/inmarsat

4.4.1.10 High Frequency (HF) Radio Communications

High frequency communications was the backbone of Coast Guard ship-shore record and tactical communications for many years. With the advent of radioteletype and data-link technology, HF provided a somewhat reliable means of passing operational and administrative traffic between mobile units and shore commands. However, many Coast Guard mission areas suffer from the lack of communications interoperability with the Navy, and potentially with international agencies which are procuring similar equipments. The Navy’s HF improvement process has inserted new HF technology into the command and control systems, including HF Automatic Link Establishment (ALE), HF High Speed Fleet Broadcast, and HF radio systems with fast tuning capabilities.

Both the Navy and the Coast Guard have documented (Data/Communications System Technical Operational Requirement, dated 1 April 1993) that the WMECs do not have the communications capability to operate effectively together. Specifically, the 210ft cutters do not have the capacity to handle large amounts of record traffic, with little or no capability of communicating in a real-time or near real-time basis. Interoperability among Coast Guard units, other law enforcement units, and DoD units is limited.

One of the most important operational requirement is for Coast Guard cutters to be interoperable with Navy ships. Cutters receiving interoperable communications capabilities must maintain interoperability with other Coast Guard units not operating with the Navy. The implications of the interoperability requirements are significant for the entire Coast Guard C4I infrastructure. The CAMS/COMMSTAs would require upgrading to provide the same capabilities that the cutters operating with the Navy have in terms of protocols, modem standards, data/message processing, data rates, and transmission security. This includes:

- Medium to high data rate serial tone modems (STMs);
- Message processing systems interoperable with Navy HF message delivery systems;
- Fast tuning, rapid frequency shift radios with ALE controllers;
- Secure voice and message communications;
- Common crypto and crypto keylists; and
- Real-time data link for command and control of own units in local and multi-national operations.

In joint or mutually supporting operations, HF communications interoperability is critical. Communications circuits must reach all users of the service being supported. To ensure interoperability, all services must use and conform to the same standards in hardware design, software application, and transmission protocols. Some of the key standards applicable to HF communications include:

- MIL-STD-188-110A - Interoperability and Performance Standards for Data Modems;
- MIL-STD-188-141A - Interoperability and Performance Standards for Medium and High Frequency Radio Equipment;
- MIL-STD-188-203-1A - Interoperability and Performance Standards for Tactical Digital Information Link; and
- MIL-STD-188-331 - Video Teleconferencing.

High data rate modems are rapidly expanding the throughput rates available on HF. Until the recent past, 75bps HF circuits were considered the “norm”. With the move to Serial Tone Modems (STMs), higher data rates were made possible due to their ability to overcome the fading problems experienced with earlier multi-tone modems. Current technology is pushing STMs to 4.8kbps with 9.6kbps expected in the near future. Technology demonstrations have shown that HF is capable of supporting data rates as high as 75kbps using satellite modems. This data rate is approaching rates that will support video transmission with the proper compression/de-compression algorithms.

Cost is a programmatic issue, but must be addressed to get the most capability for a given amount of money available. In HF communications one of the ways costs are being addressed is on a per circuit basis. This appears to be a reasonable approach, provided the definition of a circuit is clear (i.e., does it include racking, installation, cabling, shock mounts, etc.). Reasonable values appear to be $60,000-120,000 per circuit less antenna, installed. The cost depends upon the technology selected and does not include such items as old equipment and cable removal, space reconfiguration, etc.

HF communications technology has made significant advances in the past ten years, providing new capabilities to systems being fielded now and showing promise for new systems to be fielded over the next five years. As a result of this new technology insertion, HF communications have again become a viable path for long-haul communications, backing up SATCOM where they overlap and providing a reliable communications path in areas where there is limited satellite coverage.

One of the highest priorities in the National strategy is to conduct all military operations as Joint operations, if only the U.S. is involved, or as combined operations, if allied or coalition forces are involved. In all cases, interoperability is the key word. The impact on Coast Guard HF is significant for the WHECs and larger WMECs that are nationalized to Navy operational control in certain war scenarios. The interoperability requirement also has an impact on all cutters and boats that could find themselves in any operation involving other services and agencies. Several HF capabilities which may meet interoperability requirements are listed below:

- Serial Tone Modems (STMs) — standard for record message traffic, except the High Speed Fleet Broadcast (HSFB). Without high speed STMs, cutters will not be able to interact with the Navy.

- HF E-mail — includes STM and KG-84 crypto interfaced to an HF radio; rapidly becoming the medium of choice for non-tactical information exchange intra-force and between ships and shore facilities;

- HF Video — PC based and can use any media, including SATCOM and HF. HF can currently support freeze-frame and slow video, graphics and interactive real-time graphics markup, facsimile, and voice support. Although currently there is no direct impact on the Coast Guard from this Navy program, in the future it could become a standard way of joint planning. If this is the case, the Coast Guard could be hampered in future operations.

- Portable RF Integrated Network (PRIN) — provides adaptive throughput to counter jamming and interference and to provide error free data. PRIN uses ALE to establish connectivity and SURENET code-combining to obtain Automated Link Maintenance. The Navy may implement PRIN. This would have an impact on Coast Guard interoperability, since a non-PRIN platform could not communicate on PRIN supported services.

(Ref: C4I Interoperability Assessment, Pg. 132-169)

There are a number of issues associated with HF usage in the Coast Guard that may require attention. This includes High Frequency Data Link (HFDL) interoperability, where the Navy's HF E-mail system could meet Coast Guard requirements. However, the Coast Guard has expressed continued concern about using an X.25 based protocol to replace HFDL, because of cutters not being able to hear each other "stepping" on each other's transmission due to HF skyway "shadowing". (This problem could be overcome if HF E-mail is used in conjunction with an ALE controller.) The advantage of this system is that it uses recognized standards, and the system configuration allows it to be easily upgraded by changing PC cards and software rather than system hardware.

4.4.1.11 Digital Modular Radio System:

Digital Modular Radio (DMR) System will satisfy tactical communications requirements in the High Frequency (HF), Very High Frequency (VHF), and Ultra High Frequency (UHF) ranges. DMR will reduce the cost of acquiring and upgrading communications systems and will increase tactical flexibility. The DMR System will migrate from stand-alone, "stovepipe" terminal systems to a modular radio comprised of flexible, software configurable hardware modules. The DMR controller will be able to command any set of these common hardware modules to perform the function of any of the separate radios that now operate in these frequency ranges. Employing common hardware modules, standards, and software will reduce the need for multiple procurements of unique terminal systems, each with their own life cycle support. This emphasis on open hardware and software architecture will reduce the cost of acquiring, fielding, maintaining, and supporting this system.

DMR will permit the tactical commander to reconfigure RF assets in accordance with changing mission needs. Each hardware module in the DMR System will be configurable and can tune and perform related functions within multiple frequency spectrums. DMR will be compatible with Automated Digital Network System (ADNS) for network control and monitoring capabilities.

In addition, the DMR System will field integrated, multiband antennas, such as the Multifunction Electromagnetic Radiating System (MERS), that will reduce topside space and weight, and will lessen ship radar cross section (RCS). In short, DMR will provide affordable, flexible, interoperable, demand adaptive communications.

(Ref: http://www.spawar.navy.mil/pmw176/swartc16.htm)

4.4.1.12 Integrated Terminal Program:

Integrated Terminal Program (ITP) will provide flexible and responsive subsystems and terminal equipment that will enable protected narrowband and wideband communications connectivity. ITP will satisfy communications requirements in the Super High Frequency (SHF), Extremely High Frequency (EHF), and Commercial SATCOM frequency bands.

This program will field a collection of military and commercial products that will evolve to further increased communications connectivity and Joint interoperability. ITP will leverage commercial terminal systems and services, such as C- and Ku-band SATCOM, Direct Broadcast Satellite (DBS) service, International Maritime Satellite (INMARSAT), and Global Broadcast

Service (GBS) to support high data rate requirements, such as intelligence, weather, live video, news, and imagery.

ITP will place emphasis on COTS/government off-the-shelf (GOTS) components and will pursue "plug and play" modular terminal configurations. As with the Automated Digital Network System (ADNS)(described below) and DMR, the use of open systems architecture and the leveraging of commercial services and technology will reduce cost and permit rapid terminal upgrades and technology insertion. ITP will ensure compatibility with ADNS for management of RF resources.

ITP will also develop and implement multifunctional antennas, such as the Low Observable Multifunction Stack, that integrate SATCOM antennas into a single lightweight structure.

In summary, ITP capabilities, integrated with ADNS and DMR, will provide adaptable, Joint interoperable, protected, and high capacity communications at less cost.

(Ref: http://www.spawar.navy.mil/pmw176/swartc16.htm)

4.4.1.13 Automated Digital Network System:

One aspect of the Coast Guard's Internetworking Architecture (dated 1 June 1993), developed by the Internetworking Architecture Tiger Team consisting of several select Coast Guard telecommunications experts, was what they called an "intelligent gateway". Its development, they believed, would be crucial to the successful implementation of the future "network-of-networks". It was considered to be the linchpin tying the fixed shore network to the mobile sea/air network (terrestrial and space-based radio networks). The intelligent gateway was expected to become the core of the "Communication Area Master Stations (CAMS) of the future". Without this, there could never be a single writer-to-reader network.

The Navy is fielding the Automated Digital Network System (ADNS) as part of the tactical DMS implementation. It appears, from all available information, that the ADNS is the intelligent gateway. The Navy is currently fielding ADNS which will be installed at the NCTAMS and aboard all ships down to their Coastal Patrol Craft by 2003. Included in this roll-out are major Coast Guard mobile units (i.e., 378s and 270s).

The ADNS will provide efficient networking and automation capabilities, and will ensure worldwide communications connectivity via the Radio Frequency (RF) communications assets included in DMR and ITP. ADNS will leverage industry accepted standards for communications routing, switching, and management and will employ COTS/GOTS hardware and software to provide timely, efficient, and seamless data delivery to and from all data user sources (Navy, Joint and Allied).

ADNS networking capabilities will allow for the sharing of scarce communications bandwidth and will reduce reliance on "stovepipe" communications systems and dedicated bandwidth allocations. ADNS will effectively "pool" communications resources and remedy the problems caused by overloading or underutilization of communications circuits. Demonstrations and exercises, such as the JWID 95, have shown that such networking capabilities can increase utilization of communications circuits by factors of 4 to 10.

The bandwidth management and technical control automation capabilities of ADNS will provide significant payoff in terms of savings in money and manpower. Adaptation and adherence to industry standard protocols will potentially afford access to any networked INTERNETProtocol (IP) application, opening up a multitude of new opportunities, including e-mail, World Wide Web (WWW), and File Transfer Protocol (FTP).

The integration of commercial standards and COTS/GOTS hardware will significantly reduce ADNS development, procurement, and maintenance costs. Overall, ADNS maximizes information transfer efficiency and provides seamless afloat/ashore voice, video and data networks for worldwide, interoperable communications.

The special communications environments of mobile users and facilities that depend on wireless communications need to be considered. These communications are subject to jamming, noise, interference, fading, multi-path and interruption, and the protocols and access methods needed to accommodate these factors.

The evolution of technology now makes possible local storage of (potentially large) archives, and an infrastructure that supports data replication capability that can formalize and implement the replication of data among sites. Thus, careful analysis of the advantages of centralized storage with remote access needs to be compared to the advantages of local data archives that are automatically synchronized by the support infrastructure. This can be particularly true for mobile facilities where data archives can be updated on a continuing basis and available for ready reference by local users. This not only provides a potential for load-leveling on the use of communications, but assures that loss of communications will not deny access to at least segments of the critical data resources.

The advantages of a combination of both methods may also be useful where a local version of the remote data-store is updated with every query response, so that at least subsequent versions of the same query (by the same or another user) can be responded to locally.

(Ref: http://www.spawar.navy.mil/pmw176/swartc16.htm)

Table 4-11: ADNS, DMRS, ITP Comparison

Automated Digital Network System	Digital Modular Radio System	Integrated Terminal Program
Leverages Commercial Products	Builds upon common hardware, software, programmable radio technology.	Leverages commercial technology
Replaces several unique sub-networks with a single network with multimedia capabilities.	Reduces cost and increases tactical flexibility.	Introduces integrated directive antenna for topside space, weight, signature reduction.
Automates all communications systems.	Fields integrated, multiband antennas.	Pursues moeular plug-and-play terminal configurations.
Reduces development, procurement, and maintenance costs.		

Ref: http://www.spawar.navy.mil/pmw176/swartc16.htm

4.4.1.14 Application of Technologies

As stated earlier, several of the technologies in this chapter may be used in a combined effort to produce a hybrid network which will meet all of the Coast Guard's current and future voice, data, video, and interoperability requirements. Careful and accurate planning will ensure success in the future.

4.5 Technology Alternatives

Throughout the previous sections of Chapter 4, we have discussed a number of technologies that will, to varying degrees, meet certain data, mobile, or interoperability communications requirements. Individually, with consideration given to capability limitations and/or operating costs, there is no specific technology that will meet all Program Manager needs. However, by carefully selecting, analyzing, and combining several technologies into one all encompassing "network-of-networks," and thus allowing them to complement and enhance each others' capabilities, we will develop a comprehensive networking solution capable of meeting all of the Coast Guard's current and future telecommunications requirements. As discussed in the Coast Guard C4I Objective Architecture and Transition Plan, it is imperative that the ability to "quickly and easily shape information into knowledge" be provided. Telecommunications is the key technology infrastructure element which enables this to occur. For this reason, the telecommunications "network of networks" must meet the general features spelled out in the Coast Guard C4I Objective Architecture and Transition Plan for C4I infrastructure. The Coast Guard "network of networks" must be flexible, configurable, and scaleable (C4I Objective Architecture and Transition Plan items 6.3.2 & 6.5).

This section of the TCP presents a high level view of several possible networking solutions. Each alternative solution is listed below in order of precedence from the most preferred alternative to the least preferred, based on our initial capabilities assessment, technology availability, and cost analysis. After a thorough review, the Coast Guard will select up to three of these alternatives for further analysis. The results of the in-depth analysis is presented in Chapter 5 of the TCP.

The technologies contained in these alternatives are based primarily on information obtained from previous sections of the TCP (i.e., Data Communications, Mobile Communications, and Interoperability). Some technologies are currently available, some are new and emerging technologies, while others may not be available soon enough to meet the requirements of this document.

Each alternative will contain a mix of data, mobile, and interoperability technologies, which together will produce a networking solution to meet all voice, data, and video communications requirements. (Note: An asterisk (*) indicates that a particular technology can be found in each of the networking alternatives.) As new and emerging technologies evolve and are implemented, it is expected that the need for older technologies will wane. This investment in new technologies is expected to result in increased capabilities and eventual savings as the older technology is phased out. Prime examples of this are the potential for combinations of new satellite and cellular voice and data communications systems to replace current terrestrial radio systems. These terrestrial radio systems have high Coast Guard owned and maintained infrastructure costs.

Table 1, on the following page, contains a list of the technologies, described in Sections 4.1, 4.2, and 4.3 of the TCP, and also a list of the communications requirements described in Chapter 3. The Table clearly shows where certain technologies will meet specific communications requirements. Keep in mind that although a given technology is capable of meeting a specific communications requirement, cost or other factors may prohibit us from using that technology in the final networking solution. At the completion of Chapter 5 of the TCP, one networking solution will be selected as the "preferred" alternative, and planning to begin transition to this alternative will begin. However, over time, as technology updates, and changes to costs occur, another alternative may become more desirable.

This Plan primarily addresses multi-mission portions of the Coast Guard Telecommunications System (CGTS). Special purpose networks, which serve as private networks for specific Programs, and are not linked directly to the CGTS, are not addressed in detail. Examples are the Communication System (COMMSYS) Network (CSN), the Navigation Network (NAVNET), the Aviation Logistics Management Information System (ALMIS), and Intelligence Program specific networks. However, it is recognized that even though these telecommunications networks provide specific services to certain special-interest groups, they may, at a later date, be integrated into the Coast Guard Telecommunications System. The predominant concern is meeting their operational requirements within the constraints of the multimission network environment.

Other systems, not listed as an integral part of the networking alternatives, such as the Defense Information System Network (DISN), were investigated as possible networking solutions during the high-level technology analysis. These systems were not considered to be viable solutions due to one or more outstanding deciding factors. These include costs, bandwidth availability concerns, priority allocation constraints, and responsiveness to Coast Guard needs.

Table 4-12: Technology vs. Requirements

TECHNOLOGY \ REQUIREMENT	One Time Data Entry	NETWORK of Networks	Form/Inform Msg Delivery	Central Data Storage & Access	Data Security	Video (1) & Imagery (2)	Interoperability	Remote Access (Dial-In)	Internal access to CG DB & Applications	Mobile Communications	Automated Chart Updates	World-wide Public Access to CG DBs	Provide Navigation Information Service	Short Range Radio Communications	Satellite Communications	Solution to Cutter Antenna Interference	User Pull	Consolidated Management Report Sys	Direction Finding Capabilities	Video Teleconferencing	Telecommuting	Open Systems Architecture	Digital Signature Standard	Telemedicine Capability	User Charge Back	Global Dial-Tone
Wide Area Networks (WANs)																										
Asynchronous Transfer Mode (ATM)	x	x	x	x		x			x				x				x	x		x	x	x		x		
Frame Relay	x	x	x	x		x2			x				x				x	x			x	x		x		
Integrated Services Digital Network (ISDN)	x	x	x	x		x		x	x				x				x	x		x	x	x		x		
Point to Point	x	x	x	x	x	x		x	x				x				x	x		x	x	x		x		
Defense Message System (DMS)		x	x		x		x																			
Commericial Satellites																										
Iridium	x	x								x	x			x	x											x
Globalstar	x	x								x	x			x	x											x
American Mobile Satellite Corporation (AMSC)	x	x	x							x	x			x	x	x										
International Maritime Satellite (INMARSAT)	x	x	x							x	x			x	x	x										
Very Small Aperture Terminal (VSAT)																										
AT&T Tridom	x	x	x			x				x				x	x	x				x		x				x
DirecPC	x	x	x			x									x		x									
Direct Broadcast Satellite		x	x				x			x					x											
Cellular Telephone																										
Cellular Digital Packet Data (CDPD)	x	x	x				x			x				x												
TDMA/CDMA/Steinbrecher Microcells	x	x	x		x		x			x				x		x						x				
CONDOR	x	x	x		x		x			x	x			x	x	x						x				
Universal Mobile Telecommunication System		x	x				x			x			x		x	x										
Global System for Mobile Communications (GSM)		x	x		x					x					x	x										x
Wireless Communications																										
Spread Spectrum Packet Radio		x	x		x	x	x			x				x												
Medium/High Frequency Communications		x	x		x		x			x			x						x							
VHF-FM							x			x				x					x							
Digital Selective Calling (DSC)														x	x				x							
NAVTEX													x	x												
SITOR			x				x			x			x	x												

Table 4-12: Technology vs. Requirements (Cont.)

TECHNOLOGY \ REQUIREMENT	One Time Data Entry	NETWORK of Networks	Form/Inform Msg Delivery	Central Data Storage & Access	Data Security	Video (1) & Imagery (2)	Interoperability	Remote Access (Dial-In)	Internal access to CG DB & Applications	Mobile Communications	Automated Chart Updates	World-wide Public Access to CG DBs	Provide Navigation Information Service	Short Range Radio Communications	Satellite Communications	Solution to Cutter Antenna Interference	User Pull	Consolidated Management Report Sys	Direction Finding Capabilities	Video Teleconferencing	Telecommuting	Open Systems Architecture	Digital Signature Standard	Telemedicine Capability	User Charge Back	Global Dial-Tone
Military Satellite Communications (MILSATCOM)																										
Defense Satellite Communications System (DSCS)		x	x				x			x																
Military Global Broadcast System (GBS)		x	x		x		x			x					x											
UHF Demand Assign Multi-Access (DAMA)		x	x				x			x					x	x										
Mini-DAMA		x	x				x			x					x	x										
Tactical DMS		x	x		x		x			x					x	x						x				
High Speed Fleet Broadcast (HSFB)		x	x		x		x			x					x	x										
Commercial Satellite Comms Inititiative (CSCI)		x	x		x		x			x					x	x										
Challenge Athena		x	x				x			x					x	x								x		
Joint Maritime Communications Strategy (JMCOMS)																										
Automated Digital Network System (ADNS)		x					x																			
Digital Modular Radio (DMR) System		x					x																			
Integrated Terminal Program (ITP)		x					x																			
Information Standards																										
Electronic Data Interchange		x	x				x			x											x	x				
Electronic Mail Exchange		x	x				x			x					x						x	x				
INTERNET		x		x				x				x	x				x				x	x				

The networking alternatives, on the following pages, are based on the Coast Guard's technology selections and Anteon Corporation's supporting recommendations. Each alternative is broken down into three major categories: data, voice, and video. The technologies are listed where they meet the requirements within each category.

4.5.1 Networking Alternative 1

Alternative 1 is a network configuration based upon proven, currently available technologies with minimum developmental risk. This configuration closely parallels the current Coast Guard Data Network (CGDN II) upgrade initiative and major DoD telecommunications architecture improvement plans.

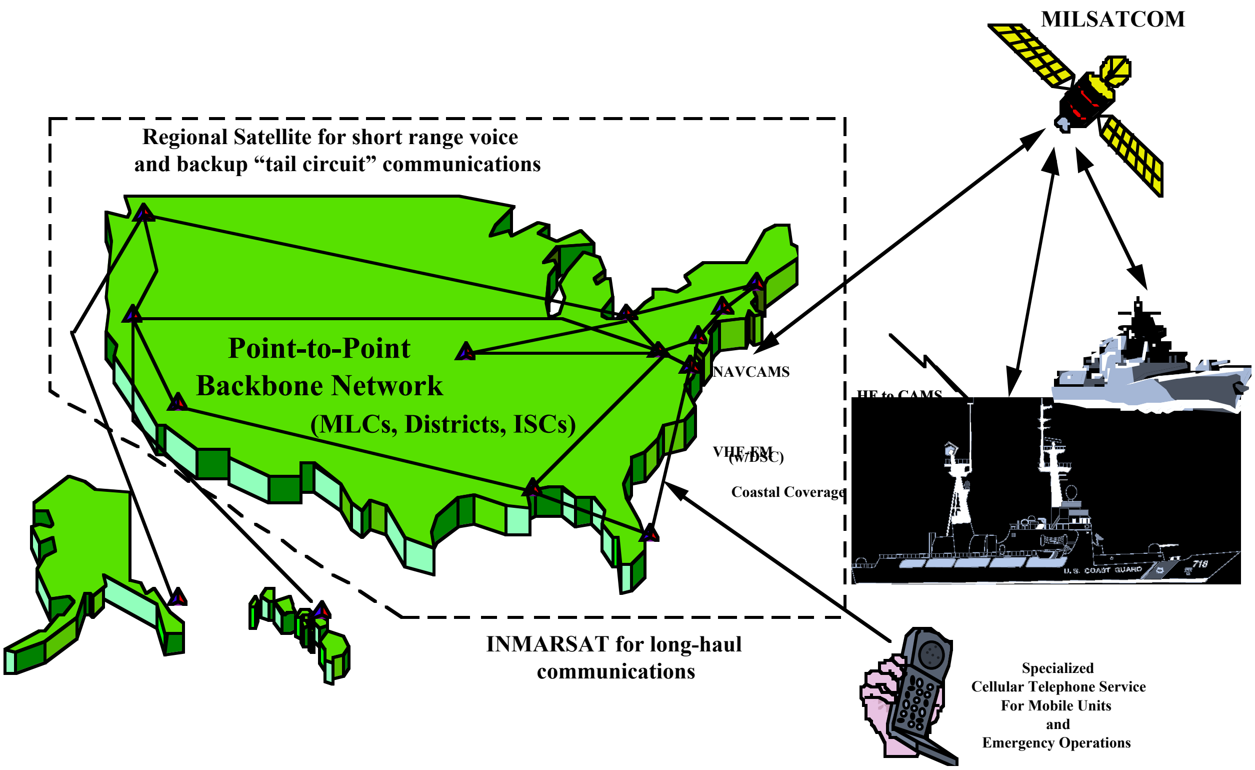


Figure 4-12: Networking Alternative #1

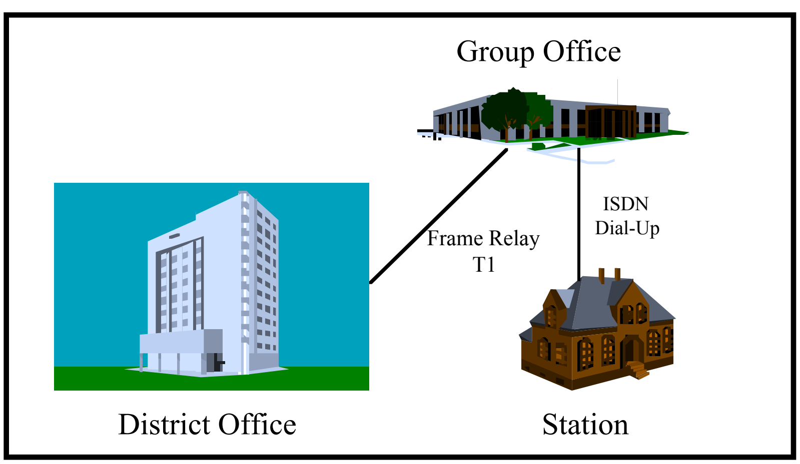


Figure 4-13: Tail Circuit

4.5.1.1 Data

The data communications portion of the Coast Guard network will consist of the following technologies:

- **Point-to-Point:** A T1, Point-to-Point backbone circuit, will use existing technology to link all major (Tier 1) Coast Guard units (i.e., Headquarters, Areas, MLCs, Districts, ISCs, AR&SC, FINCEN, TRACEN Petaluma, OSC Martinsburg, and other select units). These units will be linked with smaller units, in their respective regional areas, via a T1 Frame Relay service (new technology) or, in some cases, dial-up services. These circuits will use Transmission Control Protocol/INTERNET Protocol (TCP/IP). All Coast Guard units will have the capability of using INTERNET Web Browser technology and protocols in an INTERNET environment which will be used to form a Coast Guard INTRANET. E-mail will be used for internal record message transfer.

- **Frame Relay:** A Frame Relay T1 Intra-Coast Guard Network will connect all large (Tier 2) Coast Guard units (i.e., Groups, MSOs, Air Stations, Smaller Headquarters Units), smaller (Tier 3) units (i.e., Stations, MSDs, Recruiting Offices), and inport mobile (Tier 4) units to the Point-to-Point T1 backbone network through the major unit nodes.

- **Dial-Up Integrated Services Digital Network (ISDN):** ISDN Dial-Up services (new technology) may be used to connect small units to large units depending on cost and needs of the unit.

- *** DMS Gateways:** Gateways will provide Coast Guard access to the Defense Message System (DMS), which is an e-mail service that will run on the Defense Information System Network (DISN). (DISN is a worldwide information transfer infrastructure which includes point-to-point transmission, switched data services, video teleconferencing, etc.) There will be three gateways which will be located at OSC Martinsburg and the two MLCs. DMS services will eventually include an extension of the initial DMS network, called tactical DMS, which will allow message delivery to mobile units (378s and 270s) via satellite communications connectivity.

- *** Military Satellite Communications (MILSATCOM):** MILSATCOM (NAVMACS II/CUDIX/DAMA/OTCIXS) will be the primary means for ship-to-shore record message delivery. It will be used for satellite DMS and non-DMS record message and tactical data, ship-to-shore and ship-to-ship services to/from major Coast Guard mobile units (378s and 270s).

- **Commercial Satellite Communications (SATCOM):** Regional Satellite Systems (e.g., American Mobile Satellite Corporation (AMSC)) will be used to provide mobile units voice and data services. This may include record messaging capabilities on a secondary basis only (primary record message service will be provided by

MILSATCOM for 378s and 270s, Coast Guard satellite broadcast (LMCG) and HF for 210s, and High Frequency Data Link for 110s). (All 210s will eventually have MILSATCOM receive capabilities, and it is expected that, as satellite communications costs decrease, 110s will shift from HFDL to commercial SATCOM services.) The primary use of commercial satellite service will be underway mobile unit access to Mission Essential Applications (i.e., FLS, SARMIS, LEIS-II, etc.) and voice communications between cutters and operational commanders.

INMARSAT Commercial Satellite services will be used by mobile units located outside of the Regional Satellite System coverage area. This may be necessary in just a few instances. Redundant systems can be minimized. SARSAT will also continue to monitor distress alerts from 121.5 MHz and 406 MHz emergency position-indicating radio beacons (EPIRB).

- **MF/HF Radio Communications:** HF radio communications systems will be used for Radioteletype (RATT) broadcasts and on-call/full-termination service, as needed, and data link (HFDL) communications services for non-satellite equipped mobile units (110s, WLBs, etc.). (HF, for Coast Guard command and control, will eventually be phased out and replaced with military or commercial SATCOM services.) It will continue to be used as a backup to satellite communications for 378s and 270s. HF interface to the public will be maintained by Simplex Teletype Over Radio (SITOR), and with HF Digital Selective Calling (DSC) capabilities which will be required on certain shore stations and cutters to comply with the Global Maritime Distress and Safety System (GMDSS). MF will continue to be used for Navigational Telex (NAVTEX) and 2MHz distress guard services for the maritime public.

- **INTERNET:** INTERNET access for the public will be provided through a single gateway located at a single site (i.e., OSC Martinsburg). A "firewall" will provide the safeguards needed to protect Coast Guard internal systems from unauthorized access. Meanwhile, Coast Guard "Home Pages" will be maintained to give the public appropriate information synopsized or extracted from service-wide databases.

4.5.1.2 Voice

- **VHF-FM:** VHF-FM radio communications will continue to be used for providing maritime information broadcasts and for meeting National Distress System (NDS) service requirements at shore units and on mobile units. It will also be used for ship-to-ship and ship-to-shore command and control communications for on-scene operations, and for maintaining interoperability with the Navy and other law enforcement agencies. VHF-FM Digital Selective Calling (DSC) service will also be provided by the Coast Guard under the GMDSS. The National Distress System modernization project is studying alternatives to VHF-FM, emerging technologies to augment or replace VHF-FM, and better interfaces to the Coast Guard Telecommunications System.

- **<u>MF/HF Radio Communications:</u>** HF radio communications will continue to provide ship-to-ship, ship-to-shore, and air-to-ground voice communications (i.e., SAR and L/E operations, etc.). As satellite communications become more available and less costly to use, HF communications may assume a back-up roll in the Coast Guard communication system. MF communications will continue to provide 2MHz distress guard services for the maritime public.

- **<u>MILSATCOM:</u>** MILSATCOM services will be used to provide tactical voice communications services for satellite equipped Coast Guard mobile units (i.e., 378s and 270s);

- **<u>Commercial SATCOM:</u>** Regional Satellite (e.g., AMSC) voice services will provide coverage of the CONUS and coastal maritime areas for shore-based and mobile Coast Guard units;

  INMARSAT telephone service will provide satellite voice communications outside of the Regional Satellite Service prime coverage areas; and

- **<u>Cellular Telephone:</u>** Specialized cellular telephone services (e.g., CONDOR capable cellular/satellite telephones) will be used for emergency communications, and administrative and operational voice communications within the CONUS and CONUS Exclusive Economic Zone (EEZ) for land-based mobile units. This service will provide an interoperable link with many other agencies. FBI, DEA, and DoD are making significant commitments to CONDOR which has capability for either covered or protected communications.

4.5.1.3 Video

- **<u>Public Switched Telephone Network (PSTN):</u>** Video requirements will be met using ISDN dial-up service via the Public Switched Telephone Network (PSTN).

Table 4-13: Networking Alternative #1

ALTERNATIVE 1 / TECHNOLOGY	REQUIREMENT	One Time Data Entry	NETWORK of Networks	Form/Inform Msg Delivery	Central Data Storage & Access	Data Security	Video (1) & Imagery (2)	Interoperability	Remote Access (Dial-In)	Internal access to CG DB & Applications	Mobile Communications	Automated Chart Updates	World-wide Public Access to CG DBs	Provide Navigation Information Service	Short Range Radio Communications	Satellite Communications	Solution to Cutter Antenna Interference	User Pull	Consolidated Management Report Sys	Direction Finding Capabilities	Video Teleconferencing	Telecommuting	Open Systems Architecture	Digital Signature Standard	Telemedicine Capability	User Charge Back	Global Dial-Tone
Wide Area Networks (WANs)																											
Frame Relay		x	x	x	x		x2			x				x				x	x			x	x		x		
Integrated Services Digital Network (ISDN)		x	x	x	x		x		x	x				x				x	x		x	x	x		x		
Point to Point		x	x	x	x	x	x		x	x				x				x	x		x	x	x		x		
Defense Message System (DMS)			x	x		x		x																			
Commericial Satellites																											
American Mobile Satellite Corporation (AMSC)		x	x	x							x	x			x	x	x										
International Maritime Satellite (INMARSAT)		x	x	x							x	x			x	x	x										
Cellular Telephone																											
CONDOR		x	x	x		x		x			x	x			x	x	x						x				
Wireless Communications																											
Medium/High Frequency Communications			x	x		x		x			x			x						x							
VHF-FM								x			x				x					x							
Digital Selective Calling (DSC)															x	x				x							
NAVTEX														x	x												
SITOR				x				x			x			x	x												
Military Satellite Communications (MILSATCOM)																											
Defense Satellite Communications System (DSCS)			x	x				x			x																
Military Global Broadcast System (GBS)			x	x		x		x			x					x							x				
UHF Demand Assign Multi-Access (DAMA)			x	x				x			x					x	x										
Mini-DAMA			x	x				x			x					x	x										
Tactical DMS			x	x		x		x			x					x	x						x				
High Speed Fleet Broadcast (HSFB)			x	x		x		x			x					x	x										
Joint Maritime Communications Strategy (JMCOMS)																											
Automated Digital Network System (ADNS)			x	x				x																			
Digital Modular Radio (DMR) System			x	x				x																			
Integrated Terminal Program (ITP)			x	x				x																			
Information Standards																											
Electronic Data Interchange			x	x				x			x											x	x				
Electronic Mail Exchange			x	x				x			x					x						x	x				
INTERNET			x		x				x				x	x				x									

4.5.2 Networking Technology 2

Alternative 2 is based upon high-probability of success technologies being deployed in the near future. These technologies are anticipated to provide significant opportunities to improve Coast Guard communications processes and meet all Coast Guard future voice, data, and video requirements.

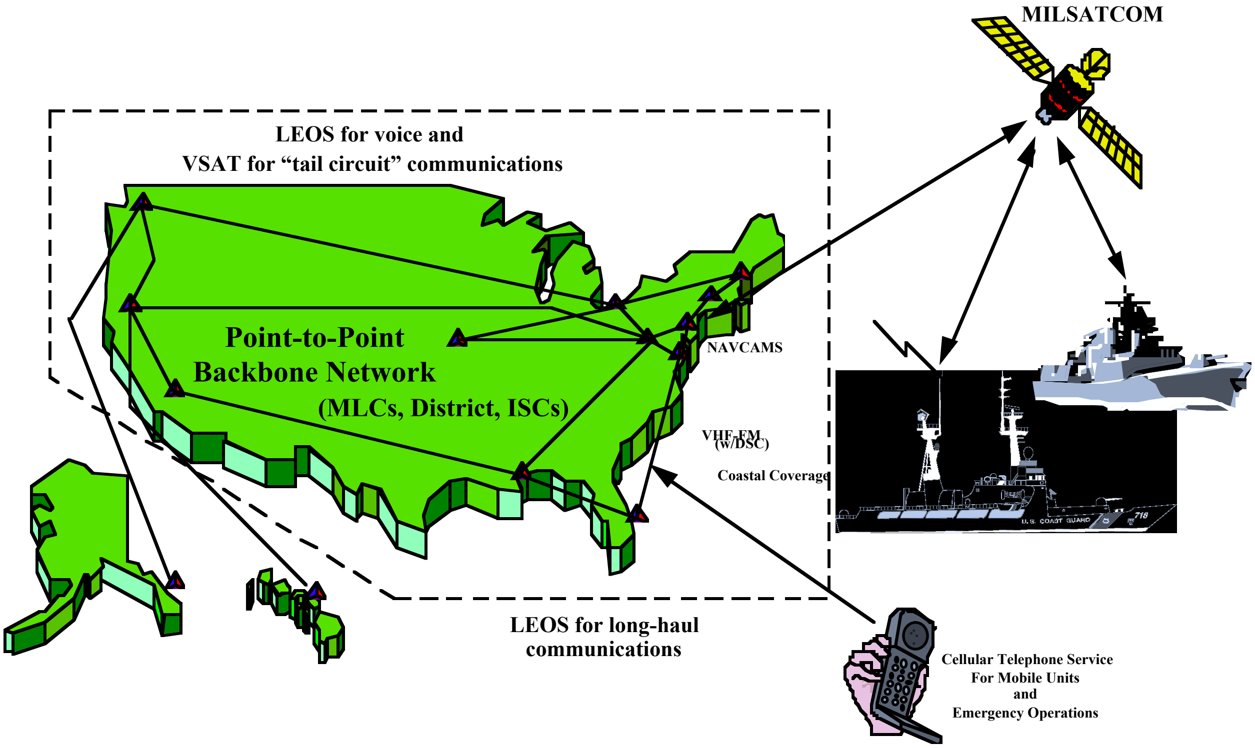


Figure 4-14: Networking Alternative #2

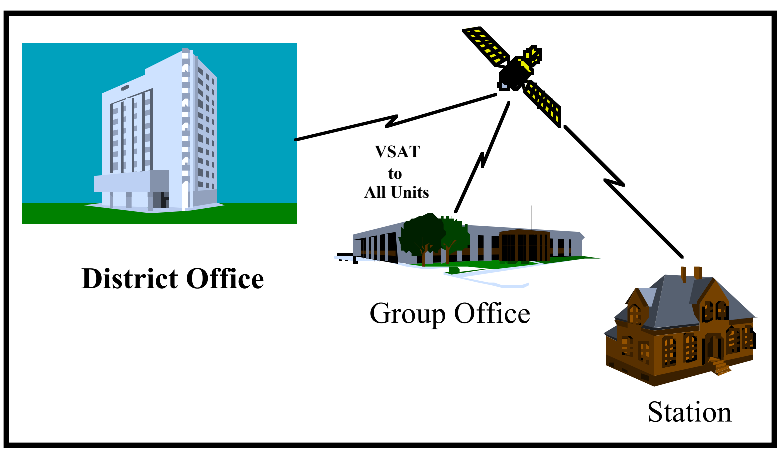


Figure 4-15: Tail Circuit

4.5.2.1 Data

- **Point-to-Point:** A T1 Point-to-Point backbone circuit, using TCP/IP, will link all Tier 1 units. These units will be linked with Tier 2 and 3 units via commercial SATCOM services. (See commercial SATCOM paragraph, below, for tail circuit architecture.) These circuits will use TCP/IP giving all units the capability of using INTERNET Web Browser technology and protocols in an INTERNET environment which will be used to form a Coast Guard INTRANET.

- **DMS Gateways:** Gateways will provide Coast Guard access to the Defense Message System (DMS), which is an e-mail service that will run on the Defense Information System Network (DISN). (DISN is a worldwide information transfer infrastructure which includes point-to-point transmission, switched data services, video teleconferencing, etc.) There will be three gateways which will be located at OSC Martinsburg and the two MLCs. DMS services will eventually include an extension of the initial DMS network, called tactical DMS, which will allow message delivery to mobile units (378s and 270s) via satellite communications connectivity.

- **MILSATCOM:** MILSATCOM (NAVMACS II/CUDIX/DAMA/OTCIXS) will be used for satellite DMS and non-DMS record message and tactical data, ship-to-shore and ship-to-ship services to/from major Coast Guard mobile units (378s and 270s);

- **Commercial SATCOM:** Very Small Aperture Terminal (VSAT) (2-way) (e.g., AT&T Tridom or Hughes DirecPC) satellite services will be used for data communications within the CONUS and CONUS Exclusive Economic Zone (EEZ). Global Low Earth Orbit Satellite (LEOS) services (e.g. IRIDIUM, Globalstar) will be used for communications outside the CONUS EEZ. This may include record messaging capabilities on a secondary basis only (primary record message service will be provided by MILSATCOM for 378s and 270s, Coast Guard satellite broadcast (LMCG) and HF for 210s, and High Frequency Data Link (HFDL for 110s). Commercial SATCOM systems are potential technologies to replace HFDL et al. However, they will need to be deployed, proven, and cost effective before a final analysis could be completed. The primary use of the commercial satellite service will be underway mobile unit access to Mission Essential Applications (i.e., FLS, SARMIS, LEIS-II, etc.) and voice communications between cutters and operational commanders.

- **MF/HF Radio Communications:** HF radio communications systems will be used for Radioteletype (RATT) broadcasts and on-call/full-termination service, as needed, and data link (HFDL) communications services for non-satellite equipped mobile units (110s, WLBs, etc.). HF interface to the public will be maintained by Simplex Teletype Over Radio (SITOR), and with HF Digital Selective Calling (DSC) capabilities which will be required on certain shore stations and cutters to comply with the GMDSS. MF will be used for Navigational Telex (NAVTEX) and 2MHz distress guard services for the maritime public.

- **INTERNET:** INTERNET access for the public will be provided through a single gateway located at a single site (i.e., OSC Martinsburg). A "firewall" will provide the safeguards needed to protect Coast Guard internal systems from unauthorized access. Meanwhile, Coast Guard "Home Pages" will be maintained to give the public appropriate information synopsized from service-wide databases.

4.5.2.2 Voice

- **VHF-FM:** VHF-FM radio communications will continue to be used for providing maritime information broadcasts and for meeting National Distress System (NDS) service requirements at shore units and on mobile units. It will also be used for ship-to-ship and ship-to-shore command and control communications for on-scene operations, and for maintaining interoperability with the Navy and other law enforcement agencies. VHF-FM Digital Selective Calling (DSC) service will also be provided by the Coast Guard under the Global Maritime Distress and Safety System (GMDSS). The National Distress System modernization project is studying alternatives to VHF-FM, and interfaces to the Coast Guard Telecommunications System will be considered.

- **MF/HF Radio Communications:** HF radio communications will continue to provide ship-to-ship, ship-to-shore, and air-to-ground voice communications (i.e., SAR and L/E operations, etc.). As satellite communications become more available and less costly to use, HF communications may assume a back-up roll in the Coast Guard communication system. MF communications will continue to provide 2MHz distress guard services for the maritime public.

- **MILSATCOM:** MILSATCOM services will be used to provide tactical voice communications services for satellite equipped Coast Guard mobile units (i.e., 378s and 270s).

- **Commercial SATCOM:** Low Earth Orbit (LEO) (new) satellite technology, such as Globalstar (or equivalent service) will be the system of choice for voice communications worldwide.

- **Cellular Telephone Service:** The existing Advanced Mobile Phone System (AMPS) cellular infrastructure will be used for emergency communications, and administrative and operational voice communications within the CONUS and CONUS Exclusive Economic Zone (EEZ) for land-based mobile units. This service may also provide interoperability with many local law enforcement agencies (i.e., FBI, DEA).

4.5.2.3 Video

- **Public Switched Telephone Network (PSTN):** Video requirements will be met using ISDN dial-up service via the Public Switched Telephone Network (PSTN)

Table 4-14: Networking Alternative #2

ALTERNATIVE 2 / TECHNOLOGY	REQUIREMENT	One Time Data Entry	NETWORK of Networks	Form/Inform Msg Delivery	Central Data Storage & Access	Data Security	Video (1) & Imagery (2)	Interoperability	Remote Access (Dial-In)	Internal access to CG DB & Applications	Mobile Communications	Automated Chart Updates	World-wide Public Access to CG DBs	Provide Navigation Information Service	Short Range Radio Communications	Satellite Communications	Solution to Cutter Antenna Interference	User Pull	Consolidated Management Report Sys	Direction Finding Capabilities	Video Teleconferencing	Telecommuting	Open Systems Architecture	Digital Signature Standard	Telemedicine Capability	User Charge Back	Global Dial-Tone
Wide Area Networks (WANs)																											
Point to Point		x	x	x	x	x	x		x	x				x				x	x		x	x	x		x		
Defense Message System (DMS)			x	x		x		x																			
Commericial Satellites																											
Globalstar		x	x								x	x			x	x											x
Very Small Aperture Terminal (VSAT)																											
DirecPC		x	x	x			x									x		x									
Cellular Telephone																											
Standard cellular			x					x			x							x									
Wireless Communications																											
Medium/High Frequency Communications			x	x		x		x			x			x					x								
VHF-FM								x			x				x				x								
Digital Selective Calling (DSC)															x	x				x							
NAVTEX														x	x												
SITOR				x				x			x			x	x												
Military Satellite Communications (MILSATCOM)																											
Defense Satellite Communications System (DSCS)			x	x				x			x																
Military Global Broadcast System (GBS)			x	x		x		x			x					x											
UHF Demand Assign Multi-Access (DAMA)			x	x				x			x					x	x										
Mini-DAMA			x	x				x			x					x	x										
Tactical DMS			x	x		x		x			x					x	x						x				
High Speed Fleet Broadcast (HSFB)			x	x		x		x			x					x	x										
Joint Maritime Communications Strategy (JMCOMS)																											
Automated Digital Network System (ADNS)			x					x																			
Digital Modular Radio (DMR) System			x					x																			
Integrated Terminal Program (ITP)			x					x																			
Information Standards																											
Electronic Data Interchange			x	x				x			x											x	x				
Electronic Mail Exchange			x	x				x			x					x						x	x				
INTERNET			x		x				x				x	x				x									

4.5.3 Networking Technology 3

Alternative 3 includes other potential high impact technologies which are available or anticipated and have not been considered in Alternative 1 or 2. In comparison to the other alternatives, Alternative 3, in using several emerging and not currently available technologies, may appear less desirable as a preferred alternative. However, in the future, this may be the network of choice, when these technologies impose less risk and better service at reduced cost.

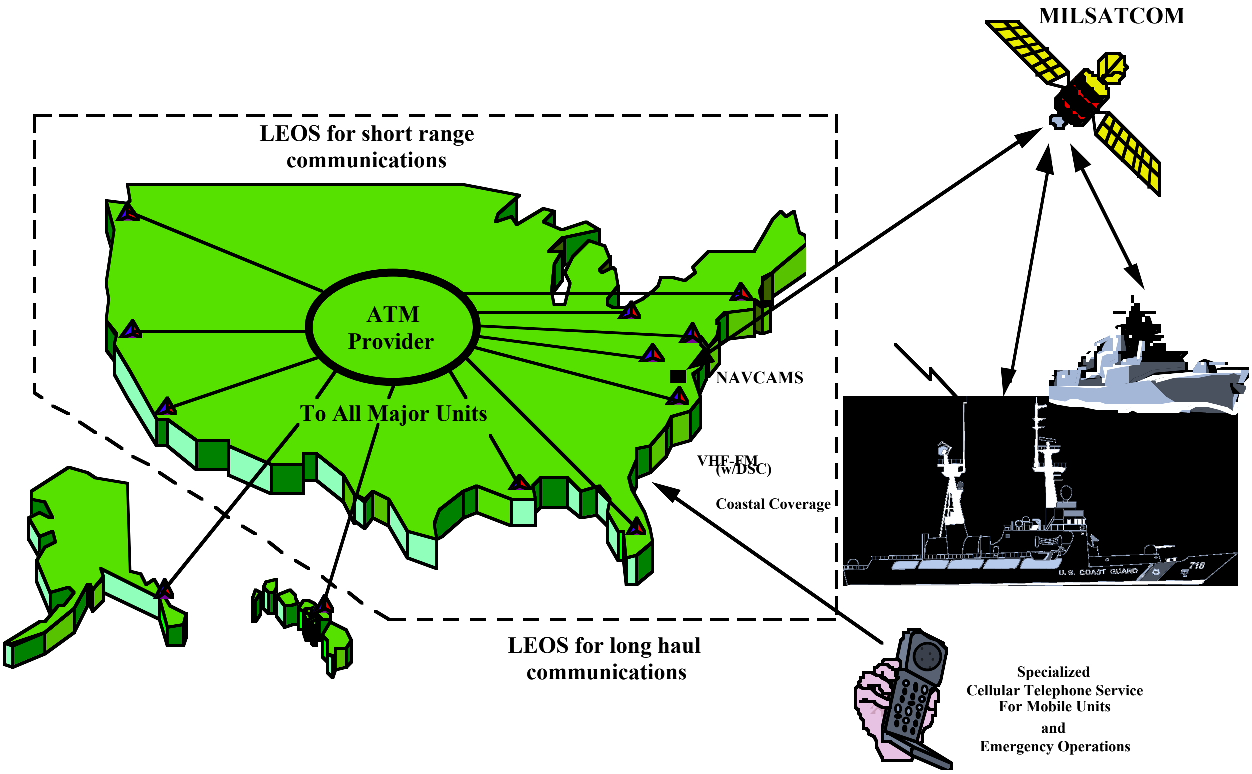


Figure 4-16: Networking Alternative #3

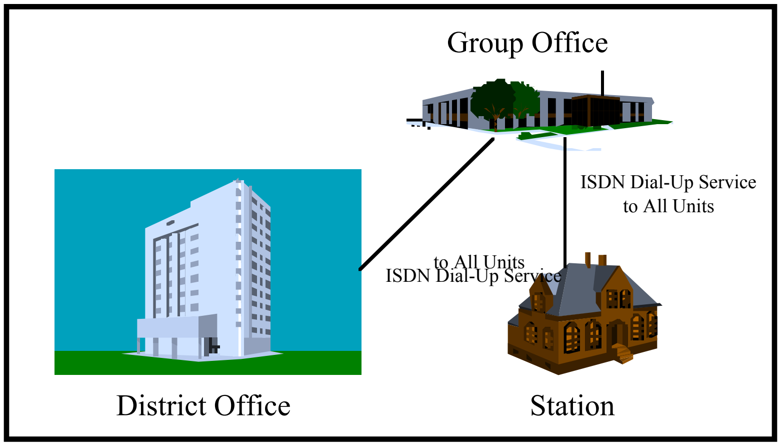


Figure 4-17: Tail Circuit

4.5.3.1 Data

The data communications portion of this networking solution will consist of the following technologies:

- **Asynchronous Transfer Mode (ATM):** An ATM T1 Backbone (emerging technology) Intra-Coast Guard Network will link all Tier 1 units. These units will be further connected to smaller (Tier 1 and 2) units, located in their respective regional areas, via ISDN Dial-Up services. All Coast Guard units will have the capability of using INTERNET Web Browser technology and protocols in an INTERNET environment which will be used to form a Coast Guard INTRANET. E-mail will be used for record message transfer;

- **ISDN Dial-Up:** ISDN services (new technology) will be used for all units at and below the Tier 1 level. Tier 2 and 3 units will connect to the ATM backbone network through the ISDN service at the Tier 1 unit nodes.

- **DMS Gateways:** Gateways will provide Coast Guard access to the Defense Message System (DMS), which is an e-mail service that will run on the Defense Information System Network (DISN). (DISN is a worldwide information transfer infrastructure which includes point-to-point transmission, switched data services, video teleconferencing, etc.) There will be three gateways which will be located at OSC Martinsburg and the two MLCs. DMS services will eventually include an extension of the initial DMS network, called tactical DMS, which will allow message delivery to mobile units (378s and 270s) via satellite communications connectivity.

- **Military Satellite Communications (MILSATCOM):** MILSATCOM (NAVMACS II/CUDIX/DAMA/OTCIXS) will be used for satellite DMS and non-DMS record message and tactical data, ship-to-shore and ship-to-ship services to/from major Coast Guard mobile units (378s and 270s);

- **<u>Commercial Satellite Communications (SATCOM):</u>** Low Earth Orbit Satellite (LEOS) services (e.g., IRIDIUM, Globalstar) will provide global voice and data coverage for mobile units. This may include record messaging capabilities on a primary basis for smaller cutters, such as 110s and WLBs, and on a secondary or tertiary basis only for larger cutters (i.e., the primary means of record message service will be MILSATCOM for 378s, 270s, and 210s). The primary use of this satellite service will be to provide underway mobile units access to Mission Essential Applications (i.e., FLS, SARMIS, LEIS-II, etc.). SARSAT will also continue be used to monitor distress alerts from 121.5 MHz and 406 MHz emergency position-indicating radio beacons (EPIRB).

- **<u>MF/HF Radio Communications:</u>** HF radio communications systems will be used for Radioteletype (RATT) broadcasts and on-call/full-termination service, as needed, and data link (HFDL) communications services for non-satellite equipped mobile units (110s, WLBs, etc.). (HF, for Coast Guard command and control, will eventually be phased out and replaced with military and/or commercial SATCOM services.) It will continue to be used as a backup to satellite communications for 378s and 270s. HF interface to the public will be maintained by Simplex Teletype Over Radio (SITOR), and with HF Digital Selective Calling (DSC) capabilities which will be required on certain shore stations and cutters to comply with the Global Maritime Distress and Safety System (GMDSS). MF will continue to be used for Navigational Telex (NAVTEX) and 2MHz distress guard services for the maritime public.

- **<u>INTERNET:</u>** INTERNET access for the public will be provided through a single gateway located at a single site (i.e., OSC Martinsburg). A “firewall” will provide the safeguards needed to protect Coast Guard internal systems from unauthorized access. Meanwhile, Coast Guard “Home Pages” will be maintained to give the public appropriate information synopsized from service-wide databases.

4.5.3.2 Voice

- **<u>VHF-FM:</u>** VHF-FM radio communications will continue to be used for providing maritime information broadcasts and for meeting National Distress System (NDS) service requirements at shore units and on mobile units. It may also continue to be the least costly means for ship-to-ship and ship-to-shore command and control communications for on-scene operations, and for maintaining interoperability with the Navy and other law enforcement agencies. Otherwise, a CONDOR capable cellular system will be used as the primary means of voice communications for Coast Guard command and control. VHF-FM Digital Selective Calling (DSC) service will also be provided by the Coast Guard under the Global Maritime Distress and Safety System (GMDSS). The National Distress System modernization project is studying alternatives to VHF-FM, and interfaces to the Coast Guard Telecommunications System will be considered.

- **<u>MF/HF Radio Communications:</u>** HF radio communications will continue to provide ship-to-ship, ship-to-shore, and air-to-ground voice communications (i.e., SAR and L/E operations, etc.). As satellite communications become more available and less costly to use, HF communications may assume a back-up roll in the Coast Guard communications system. MF communications will continue to provide 2MHz distress guard services for the maritime public.

- **<u>MILSATCOM:</u>** MILSATCOM services will be used to provide tactical voice communications services for satellite equipped Coast Guard mobile units (i.e., 378s and 270s).

- **<u>Commercial SATCOM:</u>** LEOS voice services (e.g., IRIDIUM, Globalstar) will provide coverage of the CONUS and coastal maritime areas for shore-based and mobile Coast Guard units. LEOSs can also be used world-wide for voice communications, as needed by mobile and shore units;

- **<u>Cellular Phone Service:</u>** Specialized cellular telephone services (e.g., CONDOR capable cellular/satellite telephones) will be used for emergency communications, and short-haul administrative and operational voice communications for land-based mobile units. This service will provide an interoperable link with many other agencies. FBI, DEA, and DoD are making significant commitments to CONDOR which has capability for either covered or protected communications.

4.5.3.3 Video

- **<u>Public Switched Telephone Network (PSTN):</u>** Video requirements will be met using ISDN dial-up service via the Public Switched Telephone Network (PSTN)

Table 4-15: Networking Alternative #3

ALTERNATIVE 3 / REQUIREMENT / TECHNOLOGY	One Time Data Entry	NETWORK of Networks	Form/Inform Msg Delivery	Central Data Storage & Access	Data Security	Video (1) & Imagery (2)	Interoperability	Remote Access (Dial-In)	Internal access to CG DB & Applications	Mobile Communications	Automated Chart Updates	World-wide Public Access to CG DBs	Provide Navigation Information Service	Short Range Radio Communications	Satellite Communications	Solution to Cutter Antenna Interference	User Pull	Consolidated Management Report Sys	Direction Finding Capabilities	Video Teleconferencing	Telecommuting	Open Systems Architecture	Digital Signature Standard	Telemedicine Capability	User Charge Back	Global Dial-Tone
Wide Area Networks (WANs)																										
Asynchronous Transfer Mode (ATM)	x	x	x	x		x			x				x				x	x		x	x	x		x		
Integrated Services Digital Network (ISDN)	x	x	x	x		x		x	x				x				x	x		x	x	x		x		
Defense Message System (DMS)		x	x		x		x																			
Commericial Satellites																										
Iridium	x	x								x	x			x	x											x
Cellular Telephone																										
Condor	x	x	x		x		x			x	x			x		x	x					x				
Wireless Communications																										
Medium/High Frequency Communications		x	x		x		x			x			x						x							
VHF-FM							x			x				x					x							
Digital Selective Calling (DSC)														x	x				x							
NAVTEX													x	x												
SITOR			x				x			x			x	x												
Military Satellite Communications (MILSATCOM)																										
Defense Satellite Communications System (DSCS)		x	x				x			x																
Military Global Broadcast System (GBS)		x	x		x		x			x					x											
UHF Demand Assign Multi-Access (DAMA)		x	x				x			x					x	x										
Mini-DAMA		x	x				x			x					x	x										
Tactical DMS		x	x		x		x			x					x	x						x				
High Speed Fleet Broadcast (HSFB)		x	x		x		x			x					x	x										
Joint Maritime Communications Strategy (JMCOMS)																										
Automated Digital Network System (ADNS)		x					x																			
Digital Modular Radio (DMR) System		x					x																			
Integrated Terminal Program (ITP)		x					x																			
Information Standards																										
Electronic Data Interchange		x	x				x			x											x	x				
Electronic Mail Exchange		x	x				x			x					x						x	x				
INTERNET		x		x				x				x	x				x									

Table 4-16 shows the technologies selected for each alternative to form a hybrid networking solution that will meet all Coast Guard voice, data, and video service requirements.

Table 4-16: Networking Alternatives

Alternative	Systems and Units	#1	#2	#3
Data	CGDN+ Tier 1 Backbone	Point-to-Point	Point-to-Point	ATM
	CGDN+ Tier 2	Frame Relay	VSAT	
	CGDN+ Tier 3/4	Dial-up ISDN	VSAT	ISDN Dial-Up
	Tactical DMS to 378's/270's, DOD trfc for all others	DMS Gateways	DMS Gateways	DMS Gateways
	Tactical/record msg trfc to 378's/270's, LMCG to 210s	MILSATCOM	MILSATCOM	MILSATCOM
	MEAs to all units	Commercial SATCOM - Regional Satellite - Inmarsat	Commercial SATCOM - VSAT - LEOS	Commercial SATCOM - LEOS
	GMDSS reqt/sat backup to mobile units, HFDL WPB/WLB	MF/HF Radio Comms	MF/HF Radio Comms	MF/HF Radio Comms
	Public	INTERNET	INTERNET	INTERNET
Voice	Shore ops/mobile, distress/C3	VHF-FM	VHF-FM	VHF-FM
	GMDSS reqt/sat backup	MF/HF Radio Comms	MF/HF Radio Comms	MF/HF Radio Comms
	Tactical voice on 378/270's	MILSATCOM	MILSATCOM	MILSATCOM
	Admin and C3 voice for shore and mobile units	Commercial SATCOM - Regional Satellite - Inmarsat	Commercial SATCOM - LEOS	Commercial SATCOM - LEOS
	Emerg, admin and C3 comms for shore and mobile units	CONDOR	Cellular Service	CONDOR
Video	All units with terrestial connection	PSTN	PSTN	PSTN

4.5.4 Summary

In this chapter of the TCP, an analysis was conducted of three technologies, selected by the Coast Guard, to determine their potential for addressing current and future requirements and their impacts on the Coast Guard's future architecture. These technologies were Data, Mobile, and Interoperability. The initial analysis was kept to a high level to present only a broad view of technologies that are available, or will be available, that may meet Coast Guard voice, data, and video requirements. From the results of this analysis, three example networking solutions were developed and presented in the final section of this Chapter. Each of these solutions will meet all current and future Coast Guard voice, data, and video requirements. However, the technologies vary in capability and cost, and range from currently available existing technologies to new and emerging technologies where future availability and costs are unknown.

The first alternative is a network configuration based primarily upon proven, currently available technologies with minimum developmental risk. It consists of several data and voice technologies that combined will meet all record message, mission essential application, and tactical communications needs. These technologies include Point-to-Point and Frame Relay technology, with ISDN dial-up capabilities where needed; and MILSATCOM, Commercial SATCOM, and traditional MF/HF for wireless communications support.

The second alternative is based upon high-probability of success technologies being deployed in the near future. (These technologies are anticipated to provide significant opportunities to improve Coast Guard communications processes.) This alternative is similar to Alternative 1, however, SATCOM is used more extensively to meet shore-side and wireless communications requirements.

The third alternative includes other potential high impact technologies, such as ATM, which are available or anticipated and have not been considered in Alternative 1 or 2.

5. RECOMMENDED FUTURE ARCHITECTURE

To improve the effectiveness of its operations, the Coast Guard is committed to the development, maintenance, and support of quality computer, communications, and electronic systems. To accomplish this, and to keep pace with rapidly changing technology, the Coast Guard is seeking to meet its Strategic Goals to provide a Coast Guard-wide framework for an integrated information and communications system and to provide world-wide connectivity/interoperability for voice and data transmission in support of all Coast Guard missions.

This change is necessary to maintain effective support for all Coast Guard Programs and the maritime public, and to remain interoperable with DoD and other government agencies. Providing the scaleability needed to meet ever increasing bandwidth demands, the new "system" is expected to be faster, more reliable, and less man-power intensive, and will, over the long-term, improve overall efficiency. The goal is to create a more cost effective and mission capable telecommunication system without degrading "customer" service.

Each of the Alternatives, presented in Chapter 4, reflect variations in telecommunications protocols, topology, transmission media, interfaces, components, and support facilities. Having carefully reviewed each of these alternatives the Coast Guard selected two networking solutions for complete analysis.

In short, the analysis considered the following elements: cost/benefit, engineering feasibility, stakeholders, resource savings, time and ease of implementation, risk, trade-off (cost/time/performance), and force field analysis (weighing issues for and against migration to a new system).

A final recommendation for a future state architecture was developed from the results of the analyses and is presented at the end of this chapter. The feasibility of using each alternative architecture is discussed below in detail.

5.1 Alternatives

The following alternatives were selected by the Coast Guard for further analysis.

5.1.1 Alternative 1

Alternative 1 includes a combination of Point-to-Point and Frame Relay networking technology, using T1 circuits running TCP/IP, for data communications, with ISDN services added to the lower tier network, where available and unique requirements dictate. Wireless communications requirements are met with a hybrid network of MILSATCOM, commercial SATCOM, and traditional MF/HF radio communications. Specialized cellular telephone services (i.e., CONDOR) will be used for high priority clear and secure voice and data communications, and will be available, as a backup, to meet operational and administrative communications requirements.

The above combination of data and voice technologies will meet all record message, e-mail, mission essential application, tactical communications, and video teleconferencing needs.

5.1.2 Alternative 2

Alternative 2 combines Point-to-Point networking technology with commercial Very Small Aperture Terminal (VSAT) SATCOM services to meet all shoreside data communications needs. Wireless communications requirements are met with MILSATCOM, commercial Low Earth Orbit Satellite (LEOS) services, and traditional MF/HF radio communications. Alternative 2 is based upon current and high-probability of success technologies being deployed by other enterprises in the near future. (These technologies are anticipated to provide significant opportunities to improve Coast Guard communications processes.) This alternative is similar to Alternative 1. However, commercial SATCOM is used more extensively, in Alternative 2, in order to meet shore-side and wireless communications requirements.

If the new systems and technologies mature as expected, Alternative 2 will meet the Coast Guard's requirements as well as Alternative 1.

5.1.3 Asynchronous Transfer Mode (ATM)

In addition to the two alternatives discussed above, ATM technology was evaluated as a possible wide area network (WAN) solution. This evaluation will be accomplished by comparing network (Tiers-1 and 2) solutions in each of the three WAN technologies.

5.2 Cost Benefit Analysis

The goal in performing cost/benefit analyses (CBA) is to provide the most efficient resource allocation possible using a systematic decision making process. Consequently, an important aspect of this acquisition decision process will be a cost benefit analysis.

A CBA is a systematic economic analysis of the relationship between the life cycle cost and the operational effectiveness of an alternative solution, and it serves as a decision tool for determining the relative advantages and disadvantages of the alternative solutions being considered.

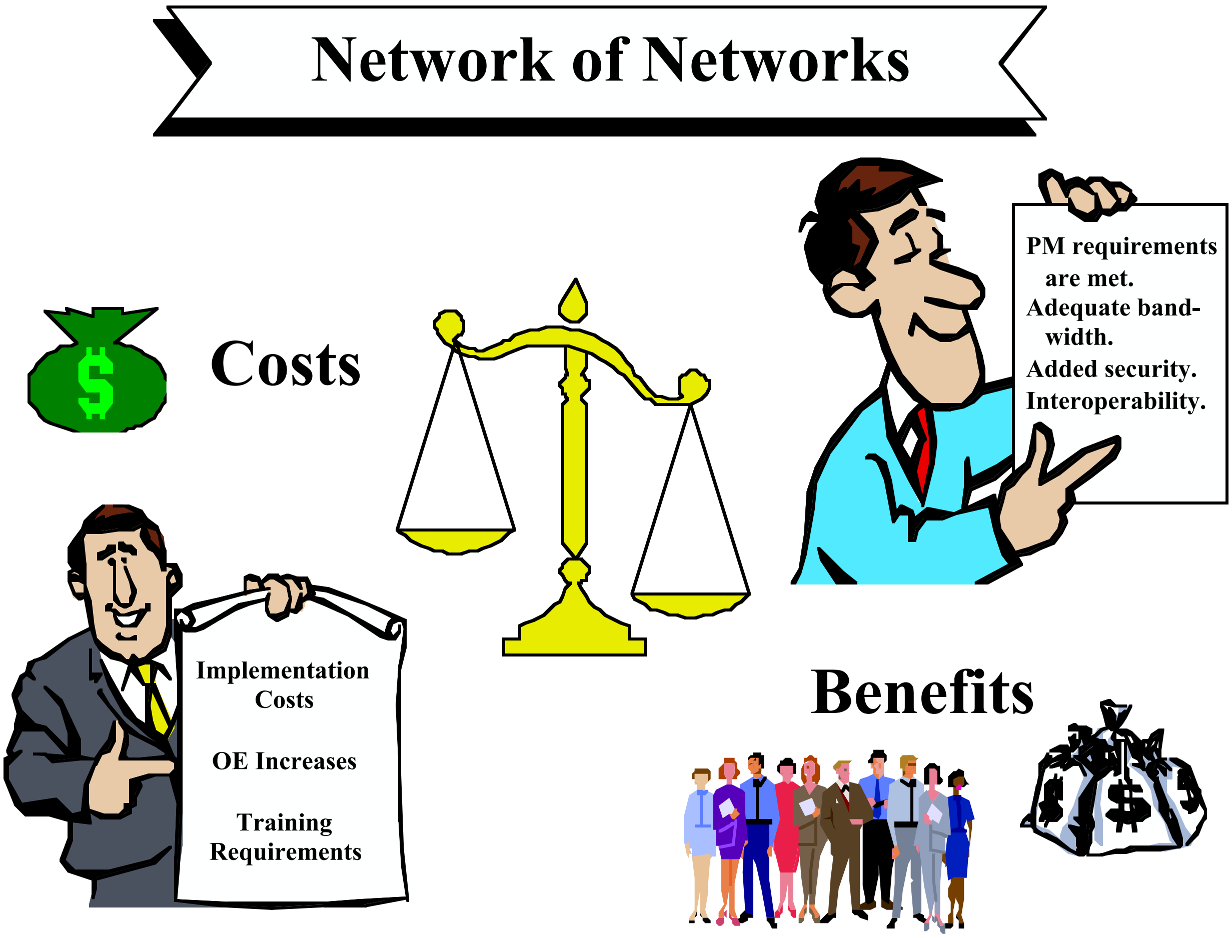


Figure 5-1: Cost vs. Benefit

5.2.1 Assumptions

In developing a cost estimate for each alternative, the following assumptions were made:

- The 5-year time period for life cycle costing of each alternatives is 1998-2002, and is appropriate for this high level analysis.
- AT&T FTS2000 price lists are applicable for Coast Guard procurements.
- Military Satellite Communications (MILSATCOM), with Defense Message System (DMS) capabilities, will be used as the primary ship-to-shore record message traffic delivery service for larger Coast Guard vessels (i.e., 378s and 270s).
- High Frequency Data Link (HFDL) will eventually be replaced by higher bandwidth, higher speed, technology (e.g. SATCOM). It will be in use for the next several years. Transition depends on the future reductions in the cost of SATCOM.

- MILSATCOM will be used by the Coast Guard for DoD tactical voice and data communications.

    To implement tactical DMS, the Navy's future Global Broadcast System (GBS) will place X-band VSAT receive terminals on all classes of ships. The operational concept is to have some bandwidth set aside for general broadcast (producer-push) and some for query services (user-pull) response. Ships will have enough bandwidth to operate like a shoreside connection. During recent tests, the Navy transmitted data over the satellite at 23 Mbps data rate.

- There is no significant charge to the Coast Guard for the use of MILSATCOM systems and equipment.

- Coast Guard can be preempted on MILSATCOM and Coast Guard specific mission communications receive a lower priority than DoD traffic.

- To keep pace with ever expanding data bandwidth requirements, the current Coast Guard Data Network (CGDN) must be replaced with a new flexible and scaleable, state-of-the-art network. If, for instance, desktop video becomes a requirement at all units, a significant increase in bandwidth will be needed and an increase in circuit costs can be expected.

- For costing purposes, network routers will be leased.

- For all mobile voice, data, and video requirements, the Coast Guard is moving toward a SATCOM solution and away from traditional radio systems (i.e. MF, HF) as a "primary" means of communications. Radio communications systems will continue to be supported as a backup for SATCOM networks in case catastrophic failure occurs (e.g., solar flare event, equipment failure, war).

    Also, radio communication systems are needed to meet SOLAS requirements. GMDSS is fielding MF/HF DSC capability to all Groups, COMMDETs, and CAMS. This will provide voice command and control capability in case catastrophic failure of SATCOM systems occur.

- Operator and maintenance training requirements will increase, for a period of time, due to the implementation of a new system.

- There will be no significant increase in the cost of traditional radio communications under the new Coast Guard Network-of-Networks.

- The Coast Guard will participate in the Global Maritime Distress and Safety System (GMDSS).

- INMARSAT installation sunk costs (current or funded) are not considered here.

- In commercial satellite systems, a one-hour per day per unit usage has been estimated for underway cutters 82’ and larger. There will be no long interactive data sessions. Ships will use data burst mode to minimize on-air time.
- In cellular systems, a one-hour per day per phone usage has been estimated.
- ISDN usage costs are $.22 per minute per channel.
- FTS2000 long distance costs are $.13 per minute.
- ISDN connect times, for Coast Guard purposes, are 5 hours per day.

Technology is not listed by vendor name in the LCCE tables for Alternatives 1 and 2. However, vendors that were used in costing these alternatives are listed by technology in Table 5-1.

Table 5-1: Vendor Names

Technology	Vendor Name
Wide Area Networks	
Point-to-Point	AT&T
Frame Relay	AT&T
ATM	AT&T
ISDN	AT&T
Commercial SATCOM	
Regional Satellite	AMSC
Global Satellite	INMARSAT
VSAT	AT&T Tridom
LEOS	GlobalStar
Cellular Service	
Standard Cellular	Cellular One
Specialized Cellular	Qualcom Corp.
Video Services	
Public Switched Telephone	AT&T

Figure 5-2 shows the Coast Guard data network hierarchy as it will likely exist under the new Network-of-Networks architecture.

5.2.2 Life Cycle Costs

The purpose of life cycle costing is to identify the total cost to the Government of a system over its useful life, including procurement, operation, support, and disposal.

LCC means total acquisition cost plus operation and support or OE costs over the life of a system.

Stated simply: LIFE CYCLE COST = TOTAL ACQUISITION COST + OE COST

The cost estimate of each alternative reflects the 5-year life-cycle cost of implementing the alternative. Beyond FY98, a yearly four percent inflation factor was used for operating cost estimation.

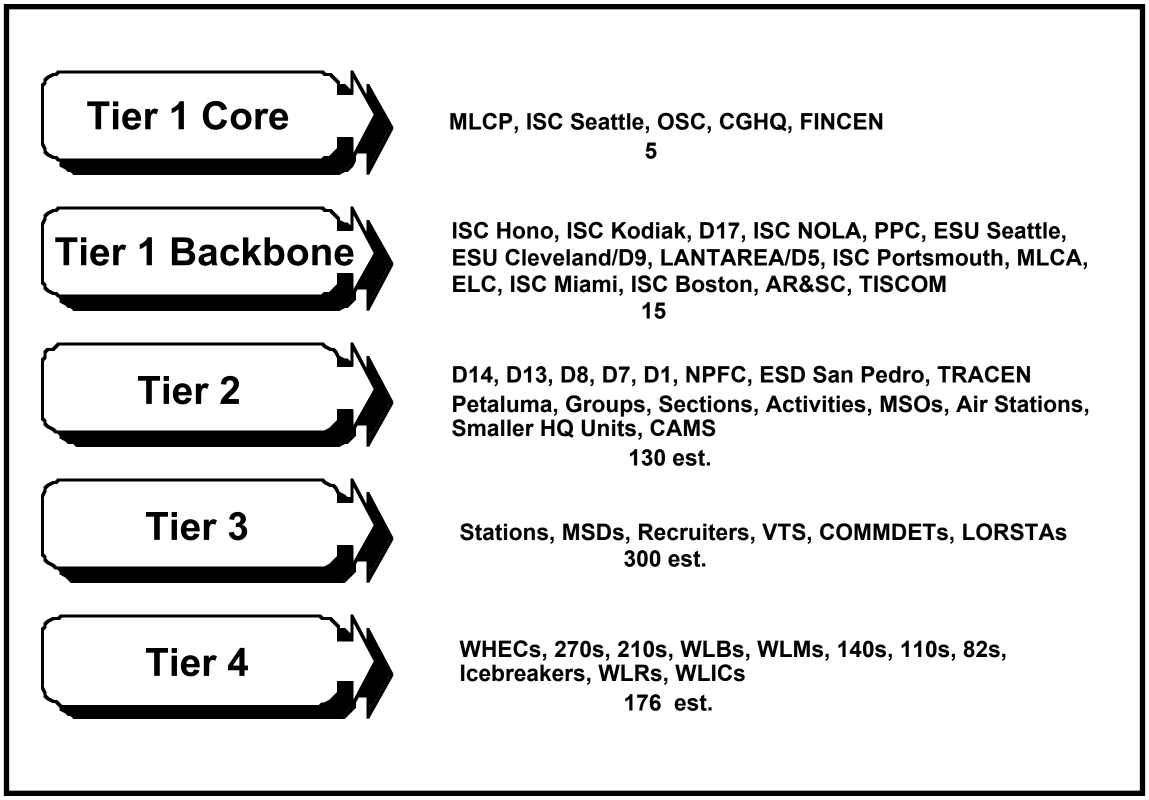


Figure 5-2: Data Network Unit Hierarchy

5.2.2.1 Alternative 1

The rough order of magnitude (ROM) LCCE, for networking Alternative 1, includes costs for equipment and installation of the equipment and circuits. Recurring cost includes the cost of operating and sustaining the network.

The LCCE was developed using Point-to-Point and Frame Relay technology to meet data service requirements for the entire Coast Guard data network down to and including Tier 3 units. ISDN costs were not included in the network design. ISDN may cover unique requirements not met by the other WAN technologies, for instance, where Frame Relay may not be available at some Tier 3 units in remote locations. Table 5-6 compares ISDN costs to the other applicable network technologies.

(Note: Frame Relay service is not available in Alaska or Hawaii. For these areas, Point-to-Point tail circuits will link Alaska and Hawaii units to a Frame Relay gateway located in Seattle, Washington and San Francisco, California, respectively.)

Regional satellite system and INMARSAT investment and recurring costs, obtained during mobile communications technology analysis, were used to develop the LCCE for commercial SATCOM services. Increased competition and technological improvements in this market are expected to further reduce the costs of satellite communications.

An LCCE for the CONDOR specialized cellular telephone capability was also included. This capability will be used for high priority voice and data communications, and for special purpose operational and administrative communications, as needed. Since this is an integrated capability of cellular and satellite, the potential exists to substitute CONDOR for standard regional and INMARSAT services.

LCCEs were developed only on those technologies that impact the go/no go decision process for a new telecommunications system. If no change in technology or cost of technology is expected, no LCCE was developed. This applies to MILSATCOM, DMS, MF/HF radio, and VHF-FM communications.

Table 5-2, below, shows the consolidated LCCE for Alternative 1. The Table shows the annual recurring and non-recurring costs of each technology. Detailed breakdowns of all LCCEs are available from G-SCT.

Table 5-2: LCCE for Alternative 1

		Recurring Costs					
Alternative 1	**non-recurring costs**	**FY 98**	**FY99**	**FY00**	**FY01**	**FY02**	**TOTAL**
Wide Area Network							
Point to Point (backbone)	$264,760	$2,477,040	$2,576,122	$2,679,166	$2,786,333	$2,897,786	$13,681,208
Frame Relay (Tiers 2 & 3)	$1,372,820	$9,441,960	$9,819,638	$10,212,424	$10,620,921	$11,045,758	$52,513,521
ISDN/FTS dial when FR N/A							
sub-total	$1,637,580	$11,919,000	$12,395,760	$12,891,590	$13,407,254	$13,943,544	$66,194,729
Commercial SATCOM							
Regional Satellite	$3,000,000	$960,000	$998,400	$1,038,336	$1,079,869	$1,123,064	$8,199,670
INMARSAT	$0	$2,079,000	$2,162,160	$2,248,646	$2,338,592	$2,432,136	$11,260,535
Specialized Cellular (CONDOR)	$2,955,000	$4,018,800	$4,179,552	$4,346,734	$4,520,603	$4,701,428	$24,722,117
Public Switched Telephone	$0	$497,640	$517,546	$538,247	$559,777	$582,168	$2,695,379
GRAND TOTALS	**$7,592,580**	**$19,474,440**	**$20,253,418**	**$21,063,554**	**$21,906,096**	**$22,782,340**	**$113,072,429**

5.2.2.2 Alternative 2

The LCCE for Alternative 2 was developed using Point-to-Point and commercial SATCOM technology (i.e., VSAT) for the entire Coast Guard data network. Point-to-Point technology will connect all Tier 1 and 2 units to the network, and VSAT will be used to connect all Tier 2 units with Tier 3 units.

Costs for standard cellular telephone capability were also included.

LCCEs were developed only on those technologies that impact the go/no go decision process for a new telecommunications system. If no change in technology or cost of technology is expected, no LCCE was developed.

Table 5-3, below, shows the consolidated LCCE for Alternative 2. The Table shows the annual recurring and non-recurring costs of each technology. A detailed breakdown of the LCCE is available from G-SCT.

Table 5-3: LCCE for Alternative 2

		Recurring Costs					
Alternative 2	**Non-recurring Costs**	**FY 98**	**FY99**	**FY00**	**FY01**	**FY02**	**TOTAL**
Wide Area Network							
Point to Point (Tiers 1 & 2)	$1,109,760	$7,289,040	$7,580,602	$7,883,826	$8,199,179	$8,527,146	$40,589,552
VSAT (Tier 3)	$2,725,000	$12,720,000	$13,228,800	$13,757,952	$14,308,270	$14,880,601	$71,620,623
sub-total	$3,834,760	$20,009,040	$20,809,402	$21,641,778	$22,507,449	$23,407,747	$112,210,175
Commercial SATCOM							
LEOS	$123,200	$817,344	$850,038	$884,039	$919,401	$956,177	$4,550,199
Standard Cellular	$98,500	$4,018,800	$4,179,552	$4,346,734	$4,520,603	$4,701,428	$21,865,617
Public Switched Telephone	$0	$497,640	$517,546	$538,247	$559,777	$582,168	$2,695,379
GRAND TOTALS	**$4,056,460**	**$25,342,824**	**$26,356,537**	**$27,410,798**	**$28,507,230**	**$29,647,520**	**$141,321,369**

5.2.2.3 Asynchronous Transfer Mode (ATM)

Table 5-4 shows a high level cost comparison between the three major networking technologies, Point-to-Point, Frame Relay, and ATM. These costs apply to Tiers-1 and 2 of the Coast Guard WAN. Comparison of these costs indicates that ATM technology, used as a WAN solution, would be more costly than Point-to-Point or Frame Relay technology.

Table 5-4: Point-to-Point, Frame Relay, ATM Comparison

		Recurring Costs					
Tier 1 & 2 Technologies	**Non-recurring Costs**	**FY 98**	**FY99**	**FY00**	**FY01**	**FY02**	**TOTALS**
Wide Area Networks							
ATM	$1,241,176	$20,149,704	$20,955,692	$21,793,920	$22,665,677	$23,572,304	**$110,378,472**
Point to Point	$1,109,760	$7,289,040	$7,580,602	$7,883,826	$8,199,179	$8,527,146	**$40,589,552**
Frame Relay	$520,726	$5,558,544	$5,780,886	$6,012,121	$6,252,606	$6,502,710	**$30,627,593**

The following bar chart, Table 5-5, is used for comparative cost analysis of the wide area networks (WANs) of each of the alternatives. These estimates are for Tiers-1 and 2 only and reflect the information in Table 5-4.

Table 5-5: Bar Chart of LCCs for Major Data Networking Alternatives

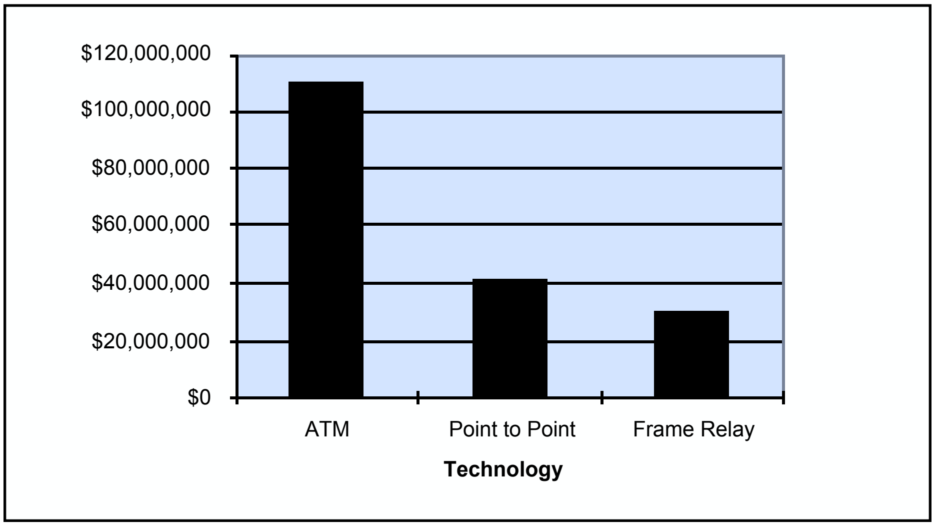


Table 5-6 shows a comparison of four technologies available for Tier 3 wide area networking. It is apparent that ISDN and VSAT are the most costly networking alternatives if used on a wide scale.

Table 5-6: Cost Comparison of ISDN, Point-to-Point, Frame Relay, and VSAT

		Recurring Costs					
Tier 3 Technologies	**Non-recurring Costs**	**FY 98**	**FY99**	**FY00**	**FY01**	**FY02**	**TOTALS**
Wide Area Networks							
ISDN	$1,674,400	$12,002,400	$12,482,496	$12,981,796	$13,501,068	$14,041,110	**$66,683,270**
Point to Point	$1,505,838	$5,928,852	$6,166,006	$6,412,646	$6,669,152	$6,935,918	**$33,618,413**
Frame Relay	$959,538	$4,055,652	$4,217,878	$4,386,593	$4,562,057	$4,744,539	**$22,926,257**
VSAT	$2,725,000	$12,720,000	$13,228,800	$13,757,952	$14,308,270	$14,880,601	**$71,620,623**

Table 5-7 is a bar chart used for comparative cost analysis of the Tier 3 WANs of each of the alternatives as reflected by the information in Table 5-6.

Table 5-7: Bar Chart of LCCs for Tier 3 Networking Alternatives

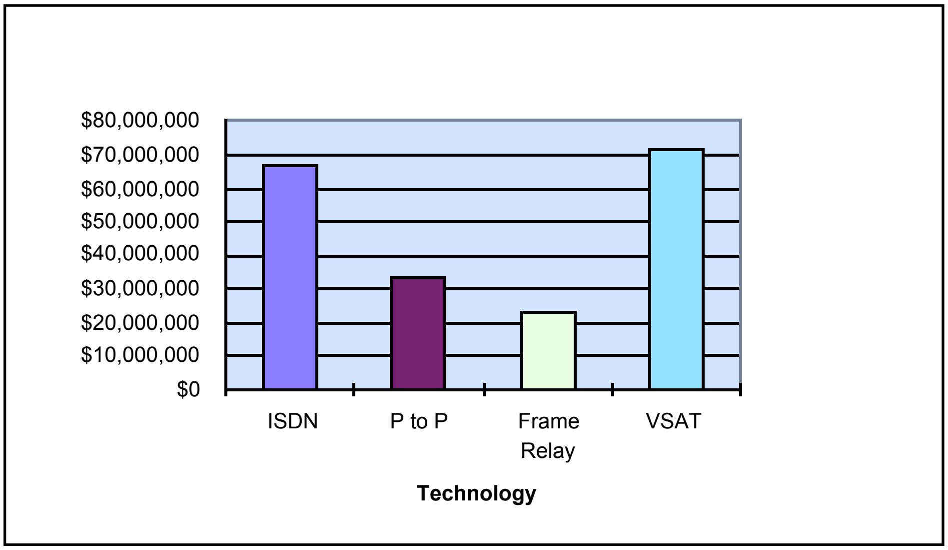


Table 5-8 shows the bandwidths that were used for the costing of the WAN alternatives. The ATM figure is the minimum bandwidth available. The bandwidths for Point-to-Point are flexible within the Point-to-Point alternative. The T1 speeds shown appear to be the best buy for the Coast Guard compared to the cost of fractional T1. Frame Relay appears to be the most scaleable of the WAN technologies. It has a broad range of committed information rates (CIR) and burst-mode options. ISDN is available in higher bandwidths than shown, in increments of 64 kbps. For VSAT, 128 kbps is the most widely used bandwidth and higher speeds are available.

Table 5-8: Delivered Bandwidth Used for Costing Alternatives

Level	Tier 1 Core	Tier 1 Backbone	Tier 2	Tier 3
Wide Area Network Technologies				
ATM	45 Mbps	45 Mbps	45 Mbps	
Point to Point	1.544 Mbps	1.544 Mbps	1.544 Mbps	1.544 Mbps
Frame Relay	384 Kbps (CIR) 1.544Mbps (burst)	384 Kbps (CIR) 1.544Mbps (burst)	128 Kbps (CIR) 512 Kbps (burst)	64 Kbps (CIR) 128 Kbps (burst)
VSAT				128Kbps
ISDN				128Kbps

5.2.3 Benefits

Several benefits will be realized from the implementation of a more cost effective and mission capable telecommunication system. The most significant benefits, resulting from selection of either of the alternatives, are described below.

5.2.3.1 Alternative 1

- Meets all the Coast Guard's communications needs. (Extensive use of multi-media to the desktop may not be possible to all units and workstations.)
- With the exception of the CONDOR cellular concept, all technologies are currently available and operational in other enterprises.
- All the technologies are still relatively young and will have presence in the communications market for many years.
- Significantly expands the bandwidth available via terrestrial WAN to levels that meet the projections of the program managers.
- Increases the Coast Guard's access to satellite systems providing more timely voice and data communications.
- CONDOR concept has significant promise for solving Coast Guard interoperability problems, since many other agencies are giving it active consideration.
- CONDOR is planned to include a seamless secure satellite/cellular link which could also reduce reliance on other satellite systems.
- Public switched telephone network (PSTN) for video teleconferencing is semi-flexible, since payment is made only for time used.

5.2.3.2 Alternative 2

- Most of the technologies are very young and will be deployed in communication systems for many years.
- Meets all the Coast Guard's communications needs. (Extensive use of multi-media to the desktop may not be possible to all units and workstations.)
- Significantly expands the bandwidth available via terrestrial WAN to levels that meet the projections of the program managers.
- Increases the Coast Guard's access to satellite systems providing more timely voice and data communications.

- Public Switched Telephone Network (PSTN) for video teleconferencing is semi-flexible, since payment is made only for time used.

5.2.4 Cost/Benefit Analysis Summary

Cost analysis shows Alternative 1 as more cost effective than Alternative 2. It also shows that the current mix of sub-alternatives may not be the best mix for the Coast Guard Network-of-Networks. The final recommended alternative combines other sub-alternatives to result in the best mix for the Coast Guard.

The analysis exposed several technologies as unreasonable within current pricing structures. ISDN, ATM, and VSAT all fall into that category. Other communications alternatives are being challenged by competition. This is especially true in the commercial satellite field.

ISDN does not appear to be an economical WAN alternative for wide use in the Coast Guard. It may be of use in situations requiring bandwidth to 128 kbps, in geographic locations without other WAN alternatives. The high cost is directly related to the amount of long distance telephone charges for virtual circuits that may require five hours of connect time per day per data channel. (Table 5-6)

ATM is only available in access speeds of 45 Mbps which overwhelmingly exceeds every projection of Coast Guard bandwidth requirements. This high bandwidth equates to high access charges, putting ATM out of cost consideration for the Coast Guard. Frame Relay and Point-to-Point were comparatively close in all tier level costing of the terrestrial WAN. (Tables 5-4 & 5-5)

VSAT is another technology that has a high price tag associated with its use. Its cost estimate was higher than any of the other alternatives for Tier 3 WAN connections. (Table 5-6)

In SATCOM, the absolute lowest cost alternatives are provided by DoD relatively free of charge, to date. If that continues to be the case, the Coast Guard should investigate every opportunity to use MILSATCOM. Previous discussion was made of Coast Guard missions having low priority on DoD networks. This must be considered in the decision process to use MILSATCOM.

Commercial SATCOM presents a diverse pricing structure. The usage charges range from $5.50 per minute (INMARSAT) down to $.30 per minute (Globalstar, plus long distance charge of $.13 per minute). This approaching tariff war has only positive ramifications for these cost estimates. Currently, the LEOS systems project has the potential to be the lowest cost alternative (Tables 5-2 & 5-3). None are operational as yet, so AMSC at $1.20/min. is the lowest cost currently available.

5.3 Engineering Feasibility

A high level engineering feasibility study was conducted to determine the availability, reliability, and engineering concerns or issues associated with the implementation of the new technology listed in Alternatives 1 and 2. The results of this study are discussed below.

The alternatives differ primarily in WAN, cellular, and satellite technology. Several of the recommended technologies are currently in use and are supported by the Coast Guard. These technologies are not expected to be a significant factor in the engineering of the new system. Therefore, those will not be discussed in any detail in this section.

A high-level migration plan is presented in Chapter 6 of this Plan. A detailed engineering and implementation plan, for the future networking architecture, will be developed by the Coast Guard.

5.3.1 Alternative 1

Alternative 1 is the “preferred” alternative of the two alternatives selected for analysis. It consists of several telecommunications service options that appear to have the least risk and/or are the most cost effective of the technologies analyzed for this Plan. These options include a combination of communications technologies that are either currently used by the Coast Guard (and will continue to be used for the foreseeable future), or are state-of-the-art, commercial off-the-shelf (COTS) technologies that will significantly enhance the current telecommunication system.

By using Point-to-Point in the core of the network, and Frame Relay in the lower Tiers, the Coast Guard will be using the two most common and available WAN technologies.

To be successful, this hybrid network of the Point-to-Point circuits and the Frame Relay Permanent Virtual Circuits (PVC) will need considerable engineering. The meshing of the network will need to be engineered in such a way as to provide sufficient bandwidth to the core Coast Guard locations.

Special attention will need to be given to the core circuits. These core circuits will support the major traffic load of the entire Coast Guard network, since the core is where the high traffic databases will be located.

- ***Point-to-Point***

  Alternative 1 uses T1 carrier Point-to-Point networking technology, running TCP/IP, as its backbone circuit connecting major Tier 1 units (i.e., Headquarters, MLCs, Districts, ISCs, TISCOM, OSC, FINCEN).

  Point-to-Point technology is an established and proven networking solution. Corporations, public and private organizations, and government agencies depend on this technology to help meet their wide area network (WAN) communications requirements.

  T1 carrier has been in use by the telephone company since the early 1960s. It was the first widely-used digital carrier. Each T1 can carry 24 voice or data channels over two copper wire pairs. T1 is based on 1.544 Mbps trunk channels which is part of the so-called digital hierarchy, and is provided over copper pairs to the local point-of presence (POP) and fiber over the long haul telephone company networks.

Because Point-to-Point technology has been in existence for many years, and its nation-wide installed base is well established and continues to grow, there is a vast source of network professionals, with a high degree of technical experience to draw from, for network support.

Point-to-Point circuits, with speeds ranging from 56 kbps to 45 Mbps, are capable of handling all current and future Coast Guard voice, data, and video requirements. It is important to keep in mind that TCP/IP does not allow "priority traffic". For this reason, scalability is crucial. If the circuits get clogged, the network needs to be flexible enough to be quickly scaled to meet the mission essential needs.

Although Point-to-Point circuits are scaleable and will provide the flexibility needed to meet all Coast Guard voice, data, and video requirements, they may not scale as quickly and easily as Frame Relay, and may be more difficult to manage.

To help reduce the risk of catastrophic failure of critical portions of the network, redundancy has been built into the system for all major Tier 1 nodes. These circuits include Headquarters, Areas, MLCs, Districts, ISCs, TISCOM, OSC, ESUs, and FINCEN. This redundancy is a key reason that the Point-to-Point system is recommended for the Tier 1 units. The Coast Guard's conservative alternate path policy ensures a reliable communications path for key mission essential applications.

- ***Frame Relay***

  In addition to the Point-to-Point circuits connecting the major backbone nodes, Alternative 1 uses Frame Relay technology to connect Tier 1 units with lower

  Tier 2, 3, and 4 units (i.e., some Districts, Groups, Air Stations, MSOs, smaller Headquarters Units, Stations, Mobile Units, etc.). Frame Relay, however, is not available in Alaska or Hawaii. For these areas, Point-to-Point tail circuits will link Alaska and Hawaii units to Frame Relay gateways located in Seattle, Washington and San Francisco, California, respectively.

  Frame Relay is a relatively new technology that scales well, is easy to manage, and is very good at efficiently handling high-speed, burst data over WANs. It can feature significantly lower costs and higher performance for those applications in contrast to the traditional Point-to-Point services. In short, Frame Relay is a proven and established technology that is considered to be a particularly fast, efficient, and reliable service.

- ***Integrated Services Digital Network (ISDN)***

  ISDN (or FTS2000 dial-up) services can be used at lower Tier units, where Basic Rate Interface (BRI) is available and as dictated by unique requirements. ISDN has been in development for over fifteen years, as the result of ever increasing digital conversion of both the network trunks and network switches for the global telephone network. It can provide the Coast Guard with a high speed circuit switched network.

- ***Specialized Cellular Capability***

  CONDOR, a specialized cellular telephone capability, can be used for high priority communications, and as a backup system for administrative and operational voice communications within the CONUS and the CONUS Exclusive Economic Zone (EEZ) for land-based mobile units. CONDOR is currently under development by the National Security Agency (NSA) and is expected to be available nation-wide in 1998.

  Initially, CONDOR is expected to be expensive in terms of development and other up-front costs. However, these costs are expected to decrease over time. CONDOR will use LEOS systems, such as Globalstar and Iridium. The LEOS system is expected to be available in 1998 for world-wide secure voice and data coverage.

  Security will be provided by FORTEZZA cryptographic cards. The cards are currently available.

Several of the network technologies, included in Alternative 1, are already being used and supported by the Coast Guard. These include MILSATCOM, cellular telephone, variations of commercial SATCOM, and traditional radio communications. Older comparable “in-service” technologies, have been included as part of the overall Network-of-Networks, in previous sections of the TCP.

All new technology, listed in Alternative 1, is commercially available or will be available in the near future.

Of the stated alternatives, Number 1 will take the least time to implement and is expected to have the least impact on Coast Guard operations and support functions. The relative maturity of the Alternative 1 technologies, and Coast Guard experience with them, provide the basis for this optimism.

5.3.2 Alternative 2

Alternative 2 has the capability to meet all Coast Guard voice, data, and video teleconferencing requirements. Like Alternative 1, it uses T1 Point-to-Point technology (discussed in 5.3.1 above), running TCP/IP, to connect all major Tier 1 and 2 units. The primary difference between this alternative and the preferred one is the use of Very Small Aperture Terminal (VSAT) technology to connect Tier 2 units with all Tier 3 and 4 units, to meet shore-side and mobile data communications requirements. Several other currently supported technologies will be used to complete the entire network.

- ***VSAT***

  Some implementations of VSAT are new on the market. They have not been thoroughly tested.

  A VSAT network is a collection of earth stations which operate in a star configuration. At the center of the star is a large central hub system and at the spokes are many remote smaller earth stations. The hub may require an antenna that is 5-6 meters in diameter or larger. The remote earth stations, on the other hand, may be as small as 1-2 meters in diameter.

  The satellite channels are currently 56-128 kbps in speed and are shared among many remote stations. One channel is broadcast from the hub to the remotes and is decoded by all remotes simultaneously, while the other channels or return path is time shared among the remotes.

  The real practical application is for data communications. This includes real-time on-line access to a central computer. Although it is technically possible for these systems to transmit voice, it is not generally practical or economical to use them for voice networking, especially if an alternative terrestrial method is available.

  VSAT has potential to provide improved communications service to small remote units with poor shoreside landline quality and units with other unique communication service problems or requirements.

Several of the network technologies, included in Alternative 2, are already being used and supported by the Coast Guard. These include MILSATCOM, standard cellular telephone, variations of commercial SATCOM, and traditional radio communications. Older "in-service" technologies have been included as part of the overall Network-of-Networks, in previous sections of the TCP. Technologies that are new, or that will otherwise impact the cost of implementation or operation of the new system, have been described.

The risk of using this alternative is considered to be higher than Alternative 1. The integration of emerging technologies with current systems is always risky. VSAT represents the highest risk, since a satellite system is being merged with an existing terrestrial WAN.

5.3.3 Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) has been touted as the next wave of sophisticated networking technology. ATM is designed to handle very high speed and disparate requirements, such as compressed digital video, data, and voice, and to carry this information over high speed fiber optic trunks. ATM can operate at speeds of 45 Mbps and higher.

ATM is a proven technology for local area networks (LANs) only. At present, there is no ATM standard for WANs, although proprietary and reduced versions of standard ATM are available. Until a standard, less expensive ATM WAN technology becomes available, the Coast Guard may not be able to take advantage of the capabilities that ATM offers.

ATM technology is new. Its availability is questionable for many locations. When ATM technology becomes standardized, it will offer high speed virtual network capabilities, with bandwidth on demand, connectionless networking.

5.4 Stakeholders

The "stakeholders" (or partners) in the new Coast Guard "Network of Networks" are, to varying degrees of ownership, all of the major Coast Guard Programs. In the early stages of the TCP development, Program Managers presented and discussed their current and future voice, data, and video requirements. These requirements include increased speed of service, INTERNET access, capability for user pull of data, and ability to store and retrieve information efficiently in a centralized data base. The needs of each Program have been carefully analyzed and considered in the planning and design of the new Coast Guard network.

The major Stakeholders, in the new Coast Guard network, are listed in Figure 5-3 below:

Tables 5-9 and 5-10 depict the level of ownership, or "stake," each Program may have in the future Coast Guard telecommunication system and in the overall networking solution. Program Managers share the need for a networking solution that will meet all of their voice, data, and video requirements with the least impact and cost to the user.

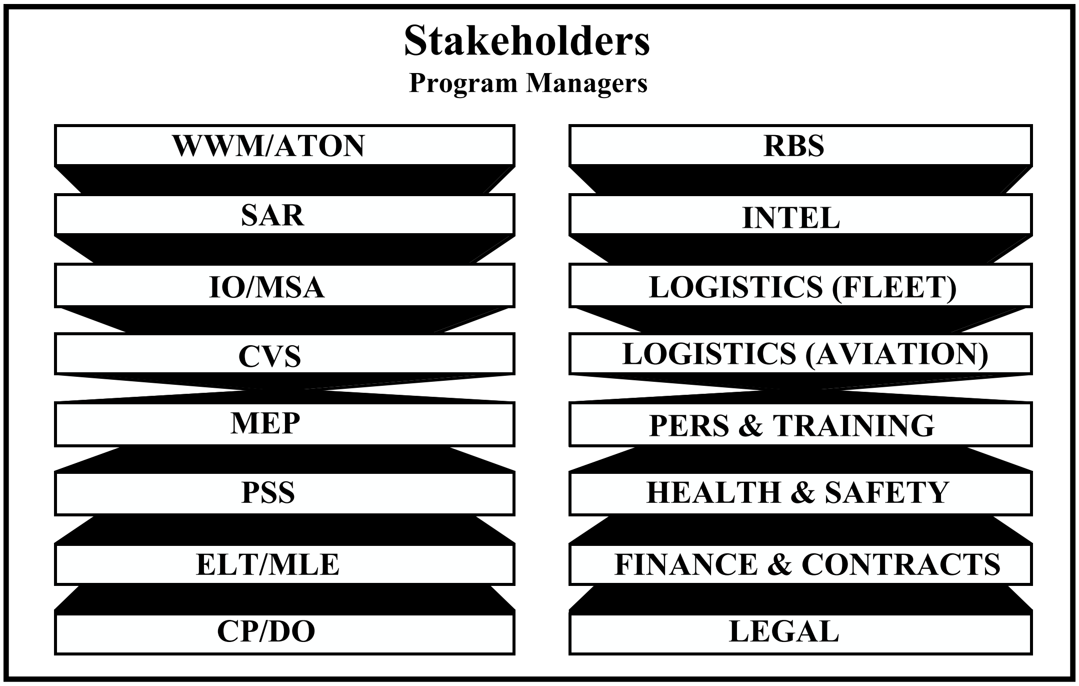


Figure 5-3: Stakeholders in the Network of Networks

These tables will be used, for planning purposes, to further examine the selected technologies, and reinforce the critical need for each one in the final networking solution. Where a block is darkened, the respective Program is projected to use that particular technology, to some degree, in meeting their mission requirements.

Table 5-9: Stakeholders - Alternative 1

Category	Alternative 1 Technologies	WWM/ATON	SAR	IO/MSA	CVS	MEP	PSS	ELT/MLE	CP/DO	RBS	Intel	Logistics (Fleet)	Logistics (Aviation)	Personnel & Training	Health & Safety	Finance & Contracts	Legal
Data	Point-to-Point	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Data	Frame Relay	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Data	Dial-Up ISDN	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Data	DMS Gateways		■	■			■	■	■	■	■	■	■		■		■
Data	MILSATCOM		■	■				■	■		■	■					■
Data	Commercial SATCOM																
Data	Regional Satellite	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■
Data	INMARSAT		■	■	■	■		■	■		■	■					
Data	MF/HF Radio Communications	■	■	■	■	■		■	■	■	■	■					
Data	INTERNET	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Voice	VHF-FM	■	■	■	■	■	■	■	■	■	■						
Voice	MF/HF Radio Communications	■	■	■	■	■		■		■	■	■					
Voice	MILSATCOM		■					■	■		■						
Voice	Commercial SATCOM																
Voice	Regional Satellite	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■
Voice	INMARSAT		■	■				■	■		■	■					
Voice	Specialized Cellular Service (CONDOR)	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Video	Public Switched Telephone Network	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

Table 5-10: Stakeholders - Alternative 2

Category	Alternative 2 Technologies	WWM/ATON	SAR	IO/MSA	CVS	MEP	PSS	ELT/MLE	CP/DO	RBS	Intel	Logistics (Fleet)	Logistics (Aviation)	Personnel & Training	Health & Safety	Finance & Contracts	Legal
Data	Point-to-Point Backbone	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Data	VSAT (Tier 2/3/4)	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Data	DMS Gateways		■	■				■	■	■	■	■	■		■		■
Data	MILSATCOM		■	■				■	■		■	■					■
Data	Commercial SATCOM																
Data	LEOS	■	■	■	■	■		■	■		■	■					
Data	MF/HF Radio Communications	■	■	■	■	■		■	■	■	■	■					
Data	INTERNET	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Voice	VHF-FM	■	■	■	■	■	■	■	■	■	■						
Voice	MF/HF Radio Communications	■	■	■	■	■		■		■	■	■					
Voice	MILSATCOM		■					■	■		■						
Voice	Commercial SATCOM																
Voice	LEOS	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■
Voice	Standard Cellular Service	■	■			■	■	■		■	■						■
Video	Public Switched Telephone Network	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

5.5 Resource Savings

Implementation of the new Network-of-Networks will yield significant improvements in the overall efficiency of the Coast Guard telecommunication system. It will increase productivity and should allow the Coast Guard to meet its ever increasing operational and administrative requirements without expanding the workforce. Improvements in meeting time-sensitive requirements will be realized through the ability to quickly and easily scale the network to meet rapidly changing user requirements. This will all be accomplished through the use of improved technology.

For example, Fleet Logistics System updates from underway units would enable the Coast Guard to manage its multi-million dollar parts inventory more efficiently. Timely access to law enforcement databases would facilitate more effective use of limited operational resources. A state-of-the-art cellular/satellite communications system that is compatible with other government agency systems will meet critical interagency operability requirements. Increased WAN bandwidth will allow large amounts of information to be shared between much more capable Coast Guard CGSWIII systems. Underway electronic chart updates could significantly reduce the requirement for paper chart portfolios onboard cutters.

Coast Guard costs have been identified as initial one-time costs that will be needed for the Network-of-Networks implementation and annual operating expenses for a 5 year period. Some of this cost will be offset by an immediate payback realized through increased productivity. Operating expenses should decline overtime as technology becomes increasingly available and more widely used. Life cycles of some systems may be longer than 5 years, but that period was selected to give a relative threshold for comparing system costs.

5.6 Implementation (time/ease of implementation)

The major acquisition process is technically complex and time consuming. Since the budget approval cycle for major acquisitions takes a minimum of two years to complete, a Resource Change Proposal (RCP) should be developed and submitted for approval as soon as possible.

The implementation of network circuits, services, and equipment can begin immediately upon approval of the necessary funding. All technology needed, under the preferred alternative, is currently available or projected to be available by the end of 1998.

With proper planning, the transition should be accomplished smoothly and will maintain the current course of evolving the network to meet Coast Guard mission needs. The new system will be compatible with the Coast Guard Standard Workstation III (CGSWIII) and with all current network applications.

Configuration management is the means through which the integrity and continuity of the design, engineering, and cost trade-off decisions are made. These technical performance, producibility, operability, testability and supportability factors are recorded, communicated and controlled by Project Managers and Facility Managers. To help ensure ease of transition, configuration management should be initiated early on in the Network implementation process.

A high level migration plan will be presented in Chapter 6.

5.7 Risk Assessment

Risk management concentrates on identifying and controlling areas or events that will result in breaching project cost, technical performance parameters, and organizational changes. It will assess potential impediments to achieving project objectives. The process involves identifying the “high” cost, organizational, and technical risk drivers and using “risk handling” techniques to reduce or control areas of risk. High risk items are those that have a high probability of occurrence and strong potential for detrimental impact, if they occur. In communications systems the highest risks concern interfaces between sub-systems. Integration of VSAT and the other commercial satellite systems offer the largest challenge here. CONDOR capability is another new area that will require both engineering and operational attention.

5.7.1 Cost Risk

Cost risk, for the preferred alternative, will be LOW. However, this does not mean that cost will not be a major issue. Significant one-time and recurring costs may be required to shift from the old system to the new network.

Affordability assessments are a significant part of key acquisition decisions. The most important cost analyses required in support of acquisition decisions are the Life Cycle Cost Estimate and Cost Benefit Analysis, discussed earlier in this section. A high-level cost analysis was conducted for estimating and evaluating expected future cost to control risk.

All of the services described in Alternative 1 are currently available, or will be available, from multiple vendor sources. Competitive pricing is available and can be readily contracted. One cost variation that may occur is a reduction in data networking and satellite communications costs over time due to advancing technology and competition. Increased usage may affect costs in the other direction, if additional bandwidth is required.

5.7.2 Technical Risk:

Technical risk, for Alternative 1, will be LOW. However, this does not mean that significant technical design work and planning will not be required for completion of the final network architecture.

Strict adherence to Federal Information Processing Standards (FIPS) and the use of COTS hardware and software will ensure that Alternative 1 technologies have the capability to interface with existing and future Coast Guard systems.

The "Network of Networks" concept, with its advanced systems communications techniques, and proven nature and prevalence of the technologies used, will provide required interfaces regardless of the owner or type of data transferred.

The specifications for the network interfaces and router vendors are standardized. There will be no unusual risk, provided a reputable vendor is chosen to provide the router equipment.

The preferred alternative satisfies all Coast Guard voice, data, and video teleconferencing requirements with less technical risk than Alternative 2. The data network design provides for recovery from single point of failure at critical nodes. Tier 3 and 4 circuits do not contain redundancy in the link design of the communications network except what is provided "in the cloud" by the long distance carriers.

Exploding bandwidth requirements may quickly outstrip original estimates especially after users see the benefit of more responsive access to the network. Alternative 1's scaleability can meet this need, but additional bandwidth has cost and will impact the cost risk of the alternative. Policy decisions on such capabilities as multi-media to the desktop have major effects on the cost.

The hybrid WAN (multiple providers) has the potential for maintenance problems. Multiple vendors compound the network/system trouble shooting process. With different maintenance providers for the workstations, network, and central computer sites, you already have a potential for significant finger pointing during service restoration. Adding multiple network providers will further complicate and add risk to operations.

5.7.3 Organizational Risk

Organizational Risk, for Alternative 1, will be LOW.

Implementation will not require significant organizational changes for either alternative. All users are the stakeholders in the system, including personnel from the highest to the lowest ranking levels within the Coast Guard. In certain cases, outside sources, such as the maritime public and other government agencies, will also be users of the "network".

The "Network of Networks" will provide access to data, text, images, databases, and graphics to all authorized users at any location, at any time. It will be an integrated, all-in-one system as opposed to a myriad of disconnected heterogeneous systems. It will require more computer skills than current systems. This can be provided by a combination of entry level and specialized training (i.e., A-Schools) and higher computer literacy of today's youth.

Resource savings will be identified through the use of a more flexible and scaleable network. Overall network efficiency will be improved, which should enable personnel to meet expanding workloads with no requirement for additional staff. The combined use of currently operated systems will result in a minimal increase of user training requirements.

5.7.4 Risk of not doing this

The Coast Guard will continue to operate the current out-dated and costly telecommunication system. The current X.25 network will not support the rapidly expanding bandwidth requirement of mission essential applications. Costs to maintain and operate the system will increase. The current system will continue to be manpower intensive and become less interoperable with DoD, other government agencies, and the maritime public. Department of Transportation (DOT) Strategic Goal 7.2 will not be met.

5.8 Trade-Off (cost/time/performance)

Trade-off analyses were performed throughout the alternatives analysis and selection process. These were used to select the configuration that best satisfies system requirements, such as performance, cost, schedule, reliability, sustainability, readiness, and maintainability. In short, the Trade-Off Study was performed to determine the most cost-effective solution and to select the best methods for platform integration.

Table 5-11, below, indicates the trade-off between cost, time, and performance between the current telecommunication system and the preferred networking alternative.

Table 5-11: Trade-Offs

Item	Cost	Time	Performance
New System	Initial one-time costs may be high. System operating costs will increase initially, but are expected to decline as circuit and technology costs decrease.	Speed of service will increase. Operator workload will decrease. Operating time will decrease.	System will be flexible and scaleable, and able to adapt quickly to changing user requirements.
Old System	Operating costs will increase as maintenance costs rise and older technology becomes more costly to obtain.	Manpower intensive system. Heavy workload requirements. Slow speed circuits. High error rates.	No longer considered state-of-the-art technology. Lacks interoperability capabilities. Considered unreliable by most users.

5.9 Force field Analysis (weighing issues for and against migration)

On the following page, Table 5-12 depicts a force field analysis of the factors for and against migration to the new Network-of-Networks. Careful review of this analysis reveals significant weight towards moving to a new and improved telecommunication system to meet current and future voice, data, and video requirements.

Table 5-12: Force Field Analysis

Force Field Analysis of Network of Networks	
FOR	**AGAINST**
Meets Program Managers' Requirements	Implementation Costs
Interoperability with DoD and OGAs	Implement User Chargeback
Technology Refreshment	Operating Costs May Increase Initially
Increased Speed of Service	Increased Training Requirements
Commonality with Other Systems	COMMCEN Function Moves to User
Improved Overall System Efficiency	Org. Resistance to Technology Change
Decrease in Operator Workload	New Technology
Flexible and Scaleable System	Technology Availability
Capability for Centralized Database	
Move Toward Global Dialtone	
Implement User Pull Technology	
State-of-the-Art Technology	
Increased Communications Security	
INTERNET Technology/Access	

5.10 Summary

Two networking alternatives were analyzed to determine the cost and engineering feasibility of future implementation. The analyses considered the following elements: cost/benefit, engineering feasibility, stakeholders, resource savings, time and ease of implementation, risk, trade-off (cost/time/performance), and force field analysis (weighing issues for and against migration to a new system).

After careful consideration of the cost and availability of selected technologies, a final recommendation for a future state architecture will be presented in chapter 6.

Each alternative included several technologies that are already in use and supported by the Coast Guard. Although these technologies are an integral part of the future network, they do not impose an impact on either the cost of implementation or the operation of the new system. Therefore, they are considered to be a "constant" factor, and were not included in the life cycle costing of the new network. Technologies that are new or will otherwise impact the cost of implementation or operation of the new system were included in the LCCE.

Alternative 1 is considered to be the preferred alternative primarily because it consists of several telecommunications service options that have the least risk and/or are the most cost effective of all technologies analyzed for this Plan. These technologies are currently available, or will become available in the future, and include Point-to-Point, Frame Relay, ISDN, and specialized cellular capability (i.e., CONDOR). The analysis determined that this alternative will take the least time to implement and will impose the least burden on Coast Guard operations and support functions.

Alternative 2 uses a combination of Point-to-Point technology and VSAT satellite services to serve as the primary arteries of the Coast Guard data network architecture. Standard cellular service is used in place of the specialized cellular service included in the preferred alternative. The analysis reveals that there is a higher risk in implementing this alternative, mainly because it contains technology (i.e. VSAT), new to the Coast Guard, that may bring with it significant interface issues (i.e., between satellite systems and the rest of the WAN). This alternative is expected to be much higher than the cost of Alternative 1.

The analysis of each of the technologies listed in both of the alternatives was closely examined. The determination was made based on cost, availability, and reliability factors concerning technologies to be included in the final networking solution. The recommended future Network-of-Networks architecture is presented in the next section of the TCP and may contain some variation of the alternatives presented for review earlier in this document.

6. FINAL RECOMMENDATIONS AND MIGRATION PLAN

This chapter describes current and future plans for improvement and modernization of the Coast Guard voice and data communication system. Migration to future systems is also discussed, at a high level, specifically for long term budget and resource planning purposes.

6.1 Final Recommendations

A final recommendation for network design was concluded after a close examination of all available technologies, and detailed discussions with Coast Guard network planners and engineers. This recommendation is based on cost, availability and reliability factors, open systems compliance, and network improvement initiatives currently in progress (i.e., Coast Guard Data Network (CGDN) Plus).

The following internetworking architecture applies to all Coast Guard mission areas and will meet all voice, data, and video requirements. This architecture was developed from detailed analysis of data, mobile, and interoperability technologies described in Chapter 4, and input received from Program Managers and key Coast Guard personnel during TCP development.

Migration to the Network-of-Networks must be carefully planned and properly executed to ensure success. Outside factors, such as on-going CGSWIII migration, the National Distress System Modernization Project, budget reduction initiatives, etc., should be considered. Changes in Program Manager telecommunications requirements will be closely tracked. However, future changes should have little influence over Network implementation strategy, since the new system will be flexible and scaleable, and fully capable of handling all increasing or decreasing Coast Guard voice, data, and video requirements.

6.2 Network Description

The architecture for the data segment of the Network-of-Networks, known as CGDN Plus, is based upon proven technologies with minimum developmental risk. It was chosen because it is currently the most flexible and scaleable network. The Point-to-Point system currently appears to be the lowest cost alternative. The assumptions used to develop the alternatives analysis in Chapter 5 were modified for the final recommendations in this chapter. The predominant change was an increase in bandwidth (CIR) requirements. (Compare Tables 5-8 and 6-2) This increase in bandwidth (CIR) resulted in Frame Relay costs expanding and consequently making Point-to-Point a less expensive alternative (see Figure 6-11). As technology changes, the network can be quickly changed to meet customer requirements. In the future, certain economies of network cost may be realized through the use of other technologies. Consequently, the final architecture may consist of a hybrid network of different technologies based on the best business case in various geographic areas. Additionally, the network which evolves will need to be compatible with efficient and effective network modeling, management, and monitoring.

Several other new technologies, which are needed to achieve the final state architecture (year 2003), such as LEOS and specialized cellular service (CONDOR), are expected to be available in 1998. However, the Coast Guard should not commit to implementing new technology until it has been thoroughly tested and operated commercially for a reasonable period of time. To allow for this, we have developed a three-phased approach to implementation of the new network.

6.2.1 Network-of-Networks–Phase I (1998)

Figure 6-1, below, shows the Phase I (1998) data network hierarchy including Tier 1 Backbone (BB) network and Tier 2, 3, and 4 (cutters in port) connectivity. Figures 6-2 and 6-3, on the following page, show the network architecture designed to meet all current and future Coast Guard Program requirements.

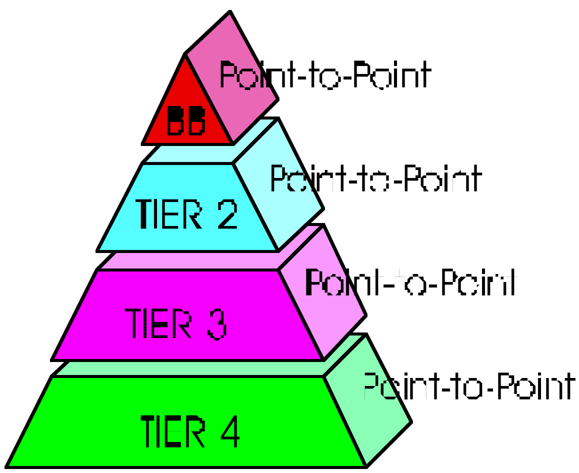


Figure 6-1: Network Hierarchy

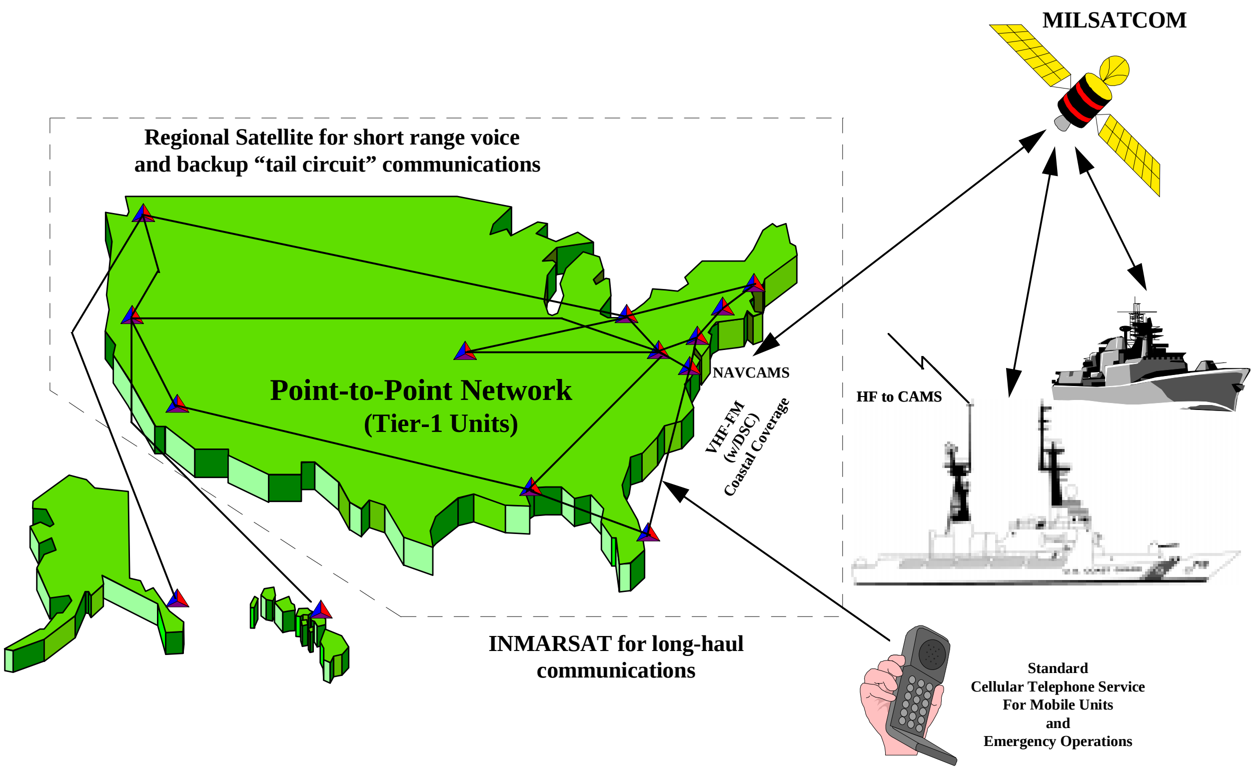


Figure 6-2: Recommended Network Architecture - Phase I

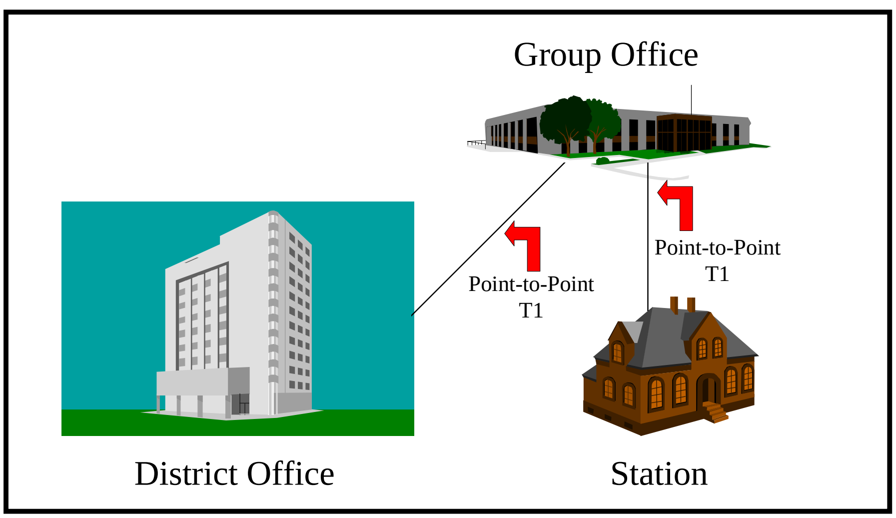
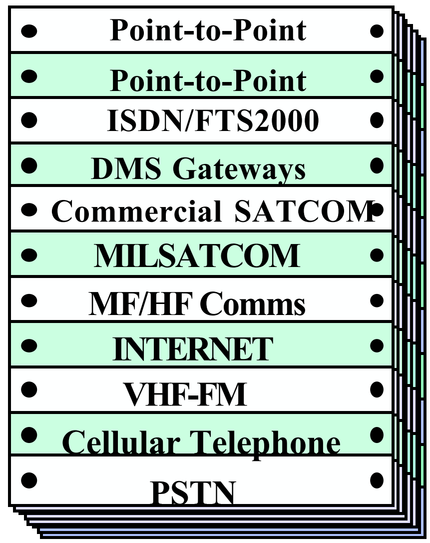


Figure 6-3: Recommended Tail Circuit Architecture

Phase I Network Description



- **Point-to-Point:** A T1, Point-to-Point backbone circuit will use existing technology to link together all major Tier 1 Coast Guard units. These units may be linked with smaller units, in their respective regional areas, via Point-to-Point circuits. In some special cases, FTS2000 or ISDN dial-up services, or other technologies, such as Frame Relay, may be used. All of these circuits will use TCP/IP, and may be assigned bandwidth depending on traffic load (i.e., T1, 56 kbps, etc.).

  With the combined use of Point-to-Point and Dial-Up services, or other available technologies, all Coast Guard units will have the capability of using INTERNET Web Browser technology and protocols in an INTERNET environment which will be used to form a Coast Guard INTRANET. E-mail will be used for internal record message transfer.

- **ISDN/FTS2000:** ISDN or FTS2000 dial-up services may be needed to cover unique Tier 2, 3, and 4 requirements not met by the Point-to-Point network, for instance, where Point-to-Point is not the most cost effective solution.

  Because of the bandwidth available on ISDN (128 kbps), it will be the first choice to be used as a substitute for Point-to-Point service. Otherwise, FTS2000 dial-up services can be used.

- **DMS Gateways:** If DMS implementation comes to fruition, gateways will provide Coast Guard access to the Defense Message System (DMS). Gateways may be located on a regional basis, one at OSC Martinsburg and one for each Area. DMS services are expected to eventually include an extension of the initial DMS network, called tactical DMS, which will allow message delivery to satellite equipped mobile units (378s, 270s, 210s). Tactical DMS connectivity may be provided to Coast Guard cutters by several means, including NAVMACS and through the Navy's Global Broadcast System (GBS) Very Small Aperture Terminal (VSAT) service.

- **Commercial SATCOM:** Regional Satellite services can provide coverage of the CONUS and coastal maritime areas for shore-based and mobile Coast Guard units.

  Currently used INMARSAT service will continue to provide satellite communications, as needed, outside of the Regional Satellite service prime coverage areas.

  Commercial SATCOM is available for ship-to-ship and ship-to-shore voice and data communications. The cost of this service may prohibit its general use for primary voice or data communications. However, its high reliability and speed of service may out weigh operating costs in meeting critical operational and/or administrative requirements.

- **Military Satellite Communications (MILSATCOM):** MILSATCOM (NAVMACS II/CUDIX S/DAMA/OTCIXS) is expected to remain (where available) the primary means for ship-to-ship record message delivery. It can be used for satellite DMS and non-DMS record message traffic and tactical data, ship-to-shore and ship-to-ship services to-from major Coast Guard mobile units (378s, 270s, 210s). Coast Guard cutters typically operate relatively independently and the Coast Guard is actively tracking the development of DMS to determine the best means of implementing DMS to the ship.

  MILSATCOM services can also be used to provide tactical voice communications services for satellite equipped Coast Guard mobile units. Another *potential* approach would be to use GBS or commercial VSAT as described below.

  > To implement tactical DMS, the Navy's future GBS may place X-band VSAT receive terminals on all classes of ships. The initial operational concept is to have some bandwidth set aside for general broadcast (producer-push) and some for query services (user-pull) response. Ships would be provided enough bandwidth to operate like a shoreside connection. During recent tests, the Navy transmitted data over the satellite with a 23 Mbps data rate. (C4I Communications Technology and Inter-Agency Interoperability Study)

- **MF/HF Radio Communications:** HF is very expensive in personnel, equipment, training, etc., and now most HF equipment seems to be near or beyond expected service life. As a result, radioteletype (RATT) broadcasts are being phased out and will be replaced with satellite communications services. On-call/full-termination RATT services will be available as a backup service for satellite equipped mobile units (378s, 270s, 210s). (HF, for Coast Guard command and control, will eventually be phased out and replaced with military or commercial SATCOM services.) As early as 1999, the Coast Guard should consider the replacement of HFDL with commercial satellite service as satellite service is fully fielded—between 2000 and 2003. HFDL should transition to a backup system as this is accomplished.

HF interface to the public will be maintained by Simplex Teletype Over Radio (SITOR) and the System Coordination Network (SCN) for voice distress guard and marine information broadcasts. Also, on the HF bands, Digital Selective Calling (DSC) capabilities will be required at certain shore stations and cutters to comply with the Global Maritime Distress and Safety System (GMDSS) requirements.

MF will continue to be used for Navigational Telex (NAVTEX) and 2 MHz distress guard services for the maritime public.

HF radio communications will continue to be available, on a limited basis, to provide ship-to-ship, ship-to-shore, and air-to-ground voice communications (i.e., SAR and L/E operations, etc.). It will also be needed for the Coast Guard to maintain Navy interoperability and for Allied communications, where satellite communications are generally not available. As satellite communications become more available and less costly to use, HF communications will likely assume a back-up role in the Coast Guard communication system. MF communications will continue to provide 2 MHz distress guard services for the maritime public.

- **INTERNET:** INTERNET access for the public may be provided through gateways located at several locations. These sites may be at Headquarters, OSC Martinsburg, and an additional site on the west coast. A "firewall" will provide the safeguards needed to protect Coast Guard internal systems from unauthorized access. Contractors only will be able to access the Coast Guard network through the firewall. Meanwhile, Coast Guard "Home Pages" will be maintained to give the public appropriate information synopsized or extracted from service-wide databases.

- **VHF-FM:** VHF-FM radio communications will continue to be used for providing maritime information broadcasts and for meeting National Distress System (NDS) service requirements at shore units and on mobile units. It may also be used for ship-to-ship and ship-to-shore command and control communications for on-scene operations, and for maintaining interoperability with the Navy and other law enforcement agencies. VHF-FM Digital Selective Calling (DSC) service will also be provided by the Coast Guard under the GMDSS.

  The on-going National Distress System Modernization Project is studying emerging technologies to provide better interfaces to the Coast Guard Telecommunication System. A Preliminary Operational Requirements Document (PORD) is currently under development in that major procurement project. Implementation of the resulting system may begin in 1999.

- **Cellular Telephone:** The existing nationwide Advanced Mobile Phone System (AMPS) cellular infrastructure can be used for high priority communications, and as a backup system for administrative and operational voice communications within the CONUS and portions of the CONUS Exclusive Economic Zone (EEZ) for land-based mobile units. Coverage in the maritime areas can vary considerably depending on proximity to population centers. This service provides an interoperable link with many other agencies.

  When specialized, dual-mode cellular service (i.e., CONDOR) becomes operational in 2000, it may be used for high priority clear and secure voice and data communications. This may include administrative and operational voice communications using LEOS systems, such as Globalstar and Iridium. As stated earlier, even though CONDOR capabilities may be available as early as 1998, the Coast Guard should not commit to implementing new technology until it has been thoroughly tested and operated commercially for a reasonable period of time.

  CONDOR capable handheld units will have dual mode capabilities. This means that each unit will have the ability to communicate via cellular or satellite systems, depending on the user's location. Each time a call is initiated, the handheld unit will first attempt to complete the call via a local cellular system. If this is not possible because the user is located outside of the cellular coverage area, CONDOR will automatically establish a reliable communications link through a LEOS system.

- **Public Switched Telephone Network (PSTN):** Video requirements will continue to be met using dial-up service via the Public Switched Telephone Network (PSTN). This can be arranged on an "as needed" basis which minimizes the recurring costs of leased lines.

6.2.2 Network-of-Networks–Phase 2 (2000)

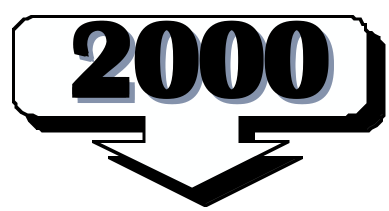


Figure 6-4, below, shows a possible networking solution for the year 2000, should the Coast Guard opt for new state-of-the-art technology. The data network hierarchy includes Tier 1 Backbone network and Tier 2, 3, and 4 (cutters in port) connectivity. Figures 6-5 and 6-6, on the following page, show the network architecture designed to meet all current and future Coast Guard Program requirements.

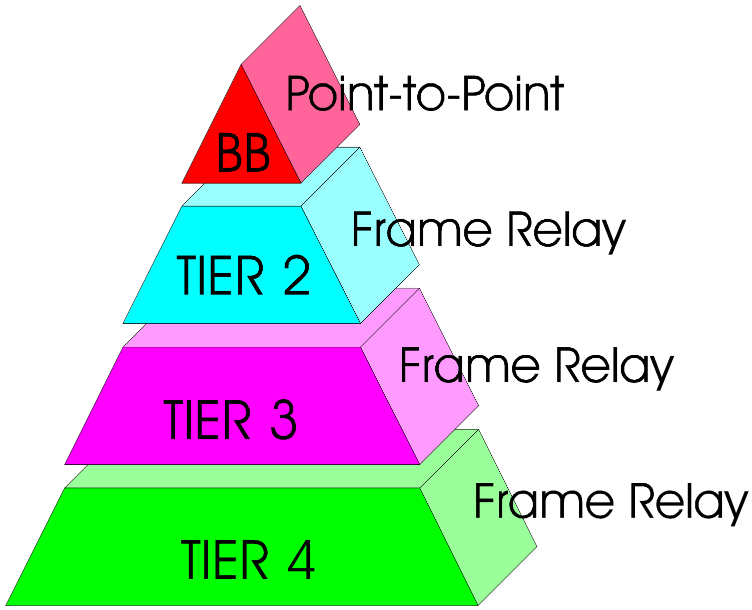


Figure 6-4: Network Hierarchy

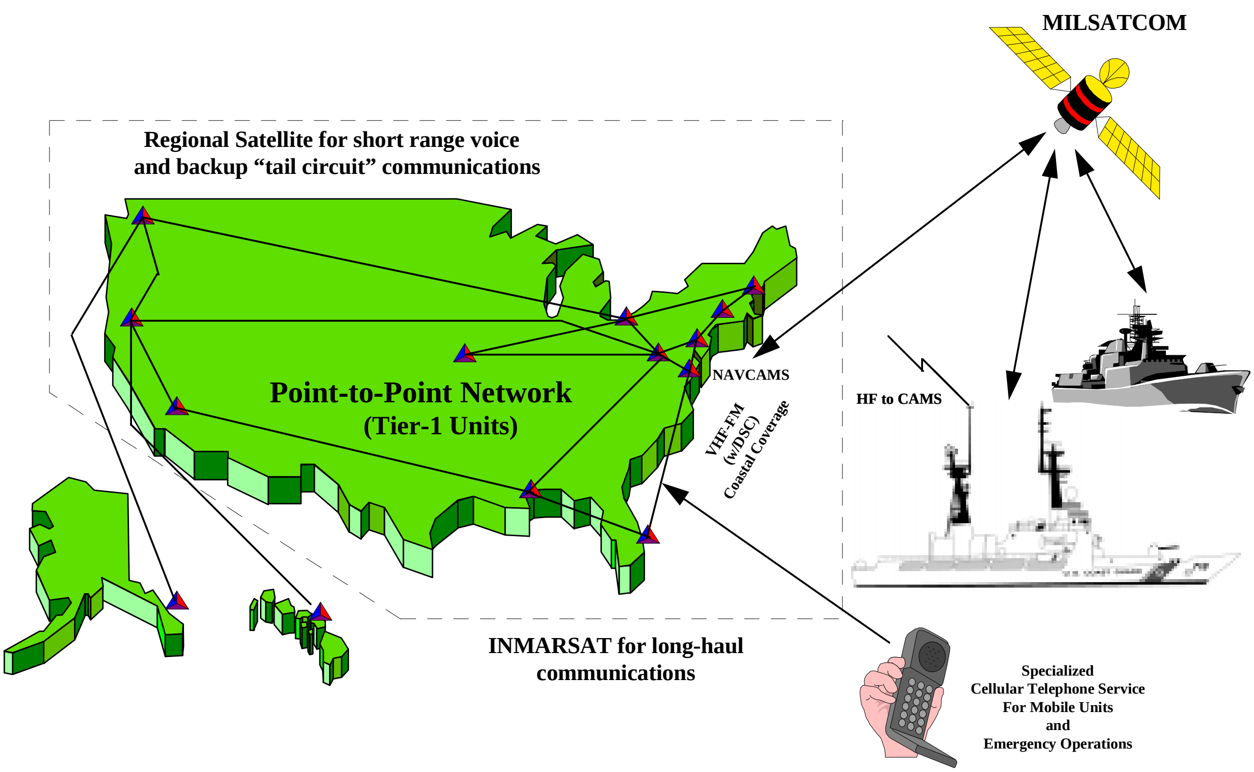


Figure 6-5: Recommended Network Architecture - Phase II

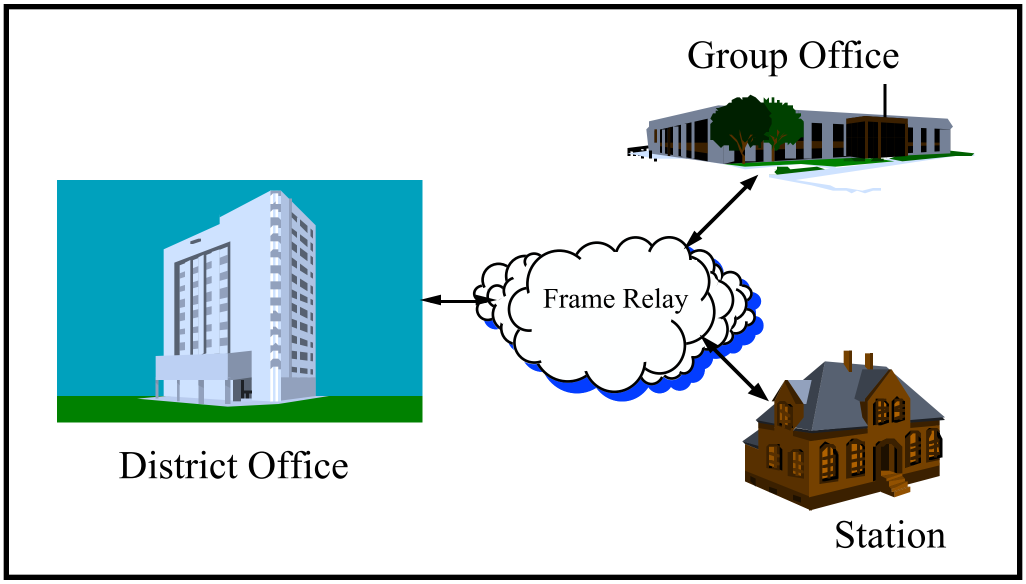
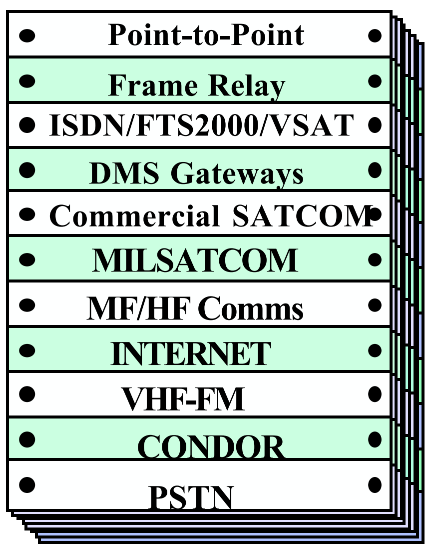


Figure 6-6: Phase II Tail Circuit Architecture

Phase II Network Description



Should the Coast Guard decide to accept Frame Relay technology as a data networking solution, in the year 2000, the following changes may be required to the Coast Guard Data Network:

- **Point-to-Point:** Under this scenario, the T1 Point-to-Point backbone circuit will continue to link together all major Tier 1 Coast Guard units. These units will be linked with smaller units, in their respective regional areas, via Frame Relay service (new technology). In some special cases, FTS2000 or ISDN dial-up services may be used. All of these circuits will use the TCP/IP protocols. With the combined Point-to-Point, Frame Relay, and Dial-Up connectivity, all Coast Guard units will continue to have the capability of using INTERNET Web Browser technology and protocols in an INTERNET environment which will be used to form a Coast Guard INTRANET. E-mail will be used for internal record message transfer.

- **Frame Relay:** A Frame Relay intra-Coast Guard network may link together all Tier 2, 3, and 4 Coast Guard units and connect them with the Point-to-Point T1 backbone network through the major unit nodes.

- **ISDN/FTS2000/VSAT:** ISDN, FTS2000 dial-up, and/or VSAT (new technology) services may be needed to cover unique Tier 2, 3, and 4 requirements not met by the Frame Relay network, for instance, where Frame Relay is not available.

  Because of the bandwidth available on ISDN (128 kbps), it may be the first choice to be used as a substitute where Frame Relay service is unavailable. Otherwise, FTS2000 dial-up services or VSAT services can be used. VSAT (AT&T Tridom) is the most costly of these options, but is fully capable of meeting Tier 2, 3, and 4 voice and data communications requirements with wireless connectivity.

- **Specialized Cellular Service:** Specialized cellular service (i.e., CONDOR) may be used in lieu of standard cellular service. Dual mode secure cellular/satellite services, with broadcast capabilities, are expected to be available from multiple vendors by the year 2000.

6.2.3 Network-of-Networks–Phase 3 (2003)

Flexibility will drive the network of the future, and it is extremely important that any future migration, towards a paperless Coast Guard, does not hurt the customer. Figure 6-7, below, shows an example networking architecture for the year 2003, which includes Tier 1 Backbone network and Tier 2, 3, and 4 (cutters in port) connectivity. This data network solution introduces Frame Relay service to the backbone circuit which completes the final stage of Frame Relay implementation to the entire Coast Guard Data Network.

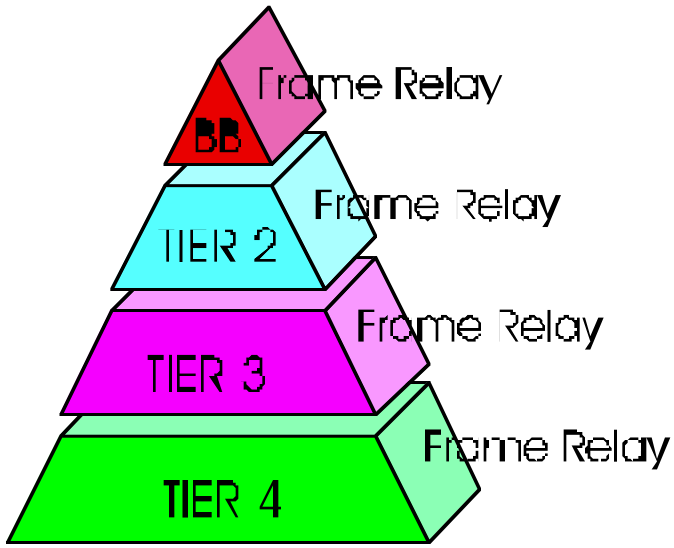


Figure 6-7: Phase III Network Hierarchy

Figures 6-8 and 6-9, on the following page, show one example of a possible final state architecture, should the Coast Guard decide to adopt Frame Relay technology as a networking solution. The selected design is an example of what may prove to be the most economical solution which provides state-of-the-art technology capable of meeting all current and future Coast Guard voice, data, and video requirements.

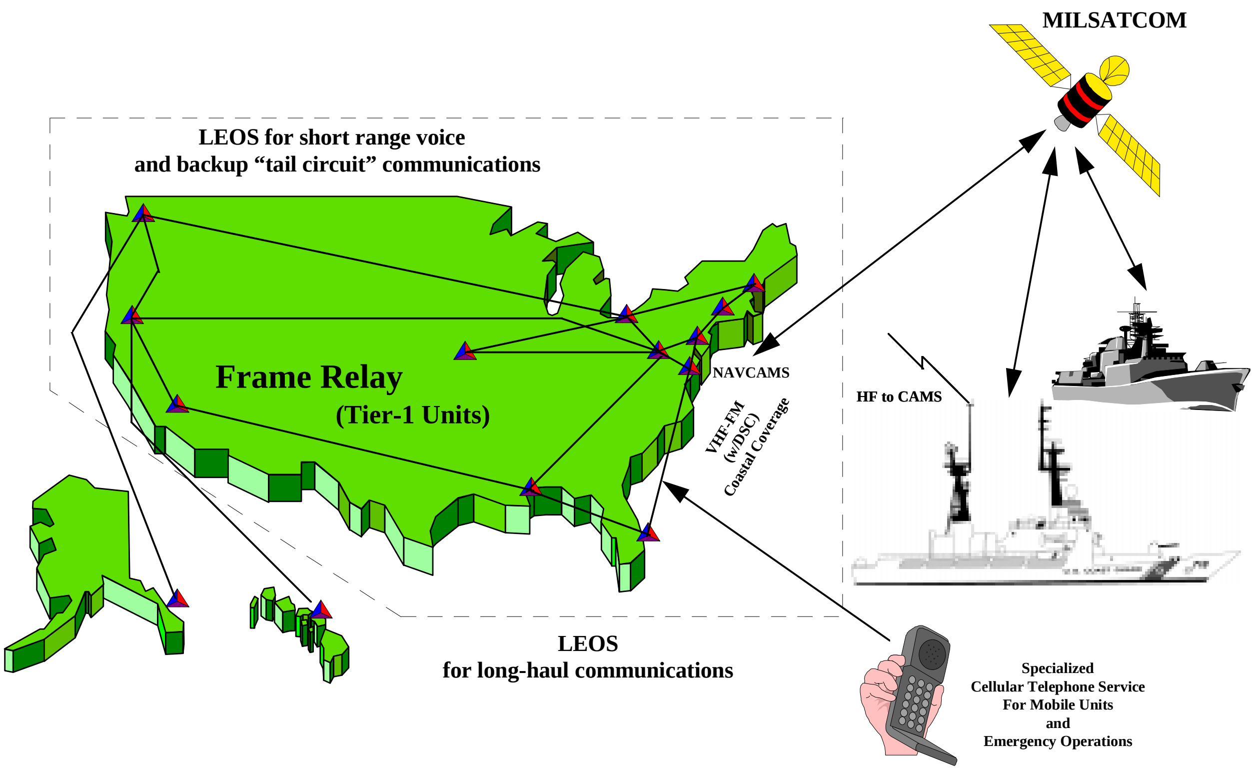


Figure 6-8: Example Network Architecture - Phase III

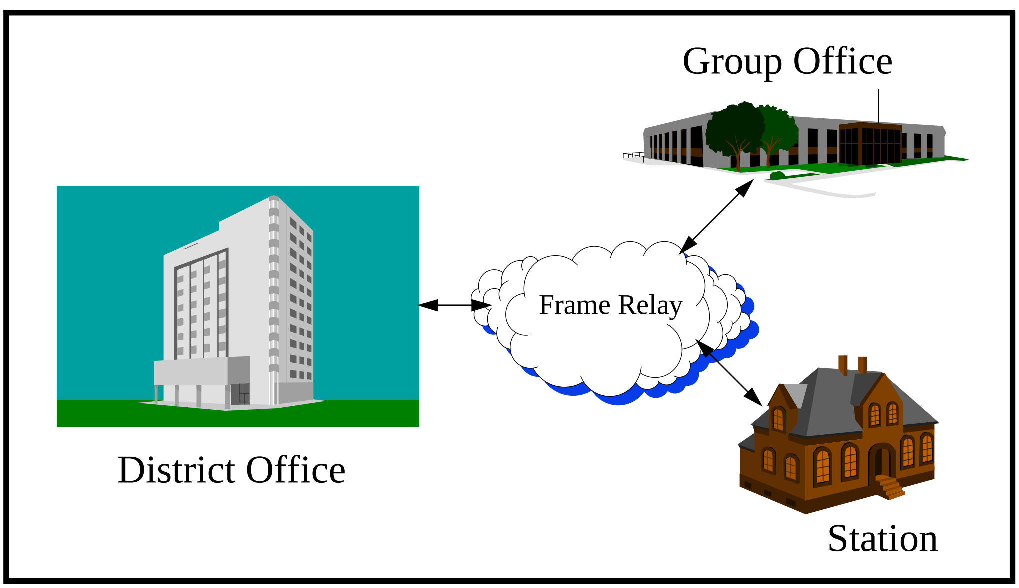
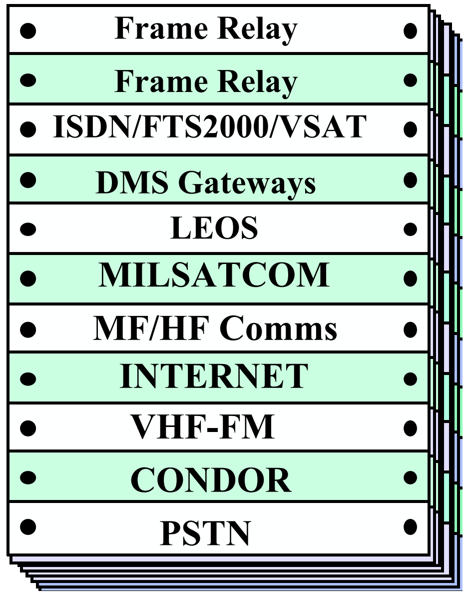


Figure 6-9: Phase III Tail Circuit Architecture

Phase III Network Description



Should the Coast Guard decide to accept Frame Relay technology, in the year 2003, as a final data networking solution, the following changes may be required to the Coast Guard Data Network. Changes in commercial satellite communications capabilities are also discussed below.

- **Frame Relay:** By the year 2003, new technology may be available and deemed to be suitable for overall network improvement, such as Frame Relay, ATM, or SONET. As with the current backbone network, the new network will link together all Tier 1, 2, 3, and 4 Coast Guard units and will allow for technology insertion which will, in turn, allow the telecommunication system to take advantage of new technology over time.

- **Commercial SATCOM:** A LEOS system may replace regional satellite and geostationary INMARSAT services for meeting special purpose mobile voice and data communications requirements. LEOS systems are expected to be thoroughly tested and operational in the commercial arena by the year 2000.

The following table shows an example of network non-recurring and recurring costs, listed by technology, for the next 6 years. Actual costs may vary should the Coast Guard opt to use different technologies in the future.

Table 6-1: Network Costs

TECHNOLOGIES	non-recurring costs	Recurring Costs FY 98	FY99	FY00	FY01	FY02	FY03	TOTAL
Wide Area Network								
Point to Point (backbone)	$270,922	$2,852,988	$2,967,108	$3,085,792	$3,209,223	$3,337,592		$15,723,62
Point to Point (Tiers 2 & 3)	$1,727,000	$6,277,800	$6,528,912					$14,533,7
Frame Relay (backbone)	$162,184						$4,687,730	$4,849,91
Frame Relay (Tiers 2 & 3 ISDN/FTS dial when FR N/	$856,768			$6,579,118	$6,842,282	$7,115,974	$7,400,612	$28,794,7
sub-total	$3,016,874	$9,130,788	$9,496,020	$9,664,909	$10,051,506	$10,453,566	$12,088,342	$63,902,0
Commercial SATCOM								
Regional Satellite	$3,000,000	$960,000	$998,400	$1,038,336	$1,079,869	$1,123,064		$8,199,67
INMARSAT	$0	$2,079,000	$2,162,160	$2,248,646	$2,338,592	$2,432,136		$11,260,5
LEOS	$123,200						$994,424	$1,117,62
Standard Cellular Service	$98,500	$4,018,800	$4,179,552					$8,296,85
CONDOR Cellular Service	$2.955.000			$4.346.734	$4.520.603	$4.701.428	$4.889.485	$21.413.2
Public Switched Telephone	$0	$497,640	$517,546	$538,247	$559,777	$582,168	$605,455	$3,300,83
GRAND TOTALS	**$9,193,574**	**$16,686,228**	**$17,353,677**	**$17,836,873**	**$18,550,348**	**$19,292,362**	**$18,577,706**	**$117,490,7**

6.3 Discussion

The example architecture provides a comprehensive networking solution capable of meeting all of the Coast Guard's current and future telecommunications requirements. It provides the ability to quickly and easily shape information into knowledge, and is designed to be flexible, configurable, and scaleable (C4I Objective Architecture and Transition Plan items 6.3.2 & 6.5).

The architecture consists of several telecommunications technologies that will best meet the Coast Guard's voice, data, and video requirements with the least cost and risk.

6.3.1 Coast Guard Data Network Plus (CGDN Plus)

The CGDN is the primary means of data communications for Coast Guard shore-side connectivity. Its use is mandated by Commandant policy, and it connects virtually every shore facility and most major cutters (in their home ports).

The Coast Guard is currently installing a new network with T1 service to most units. This will significantly increase circuit capacity available to users. The result is a much needed increase in circuit speed and improved response time for mission essential applications, such as Marine Safety Information System (MSIS), Marine Information System and Law Enforcement (MISLE), and e-mail. The new network is being carefully planned and coordinated by TISCOM to run on a "just in time" basis with CGSWIII installation efforts.

The network architecture provides Point-to-Point T1 WAN connectivity to all Tier 1 units, and may eventually extend T1 service down to the Tier 3 and 4 level. Other services may also be used, including ISDN or FTS2000 dial-up service, or even Frame Relay service, if it is deemed cost effective to do so and open systems requirements can be met.

Open systems technology and cost were the primary drivers in the choice of Point-to-Point service over other transmission technologies (i.e., Frame Relay, ATM, SONET, etc.). Frame Relay costs were found to be higher than Point-to-Point service, and additional up-front engineering of the network, under this new technology, would be required. The figures were based on similar bandwidths. If a unit's needs are less than T-1 capacity, Frame Relay can become more cost effective than Point-to-Point circuits. ATM is considerably more expensive than both Frame Relay and Point-to-Point.

TISCOM has elected to use an existing FAA sponsored government technology and services contract for CGDN Plus implementation, operation, and maintenance. This was recommended by Vice President Gore's National Performance Review (NPR) to be the network of choice for all DOT modals. This has allowed for a rapid network deployment.

Figure 6-10 shows that the cost of the network is expected to increase as more circuit capacity is needed to meet current and future Program Manager voice, data, and video requirement.

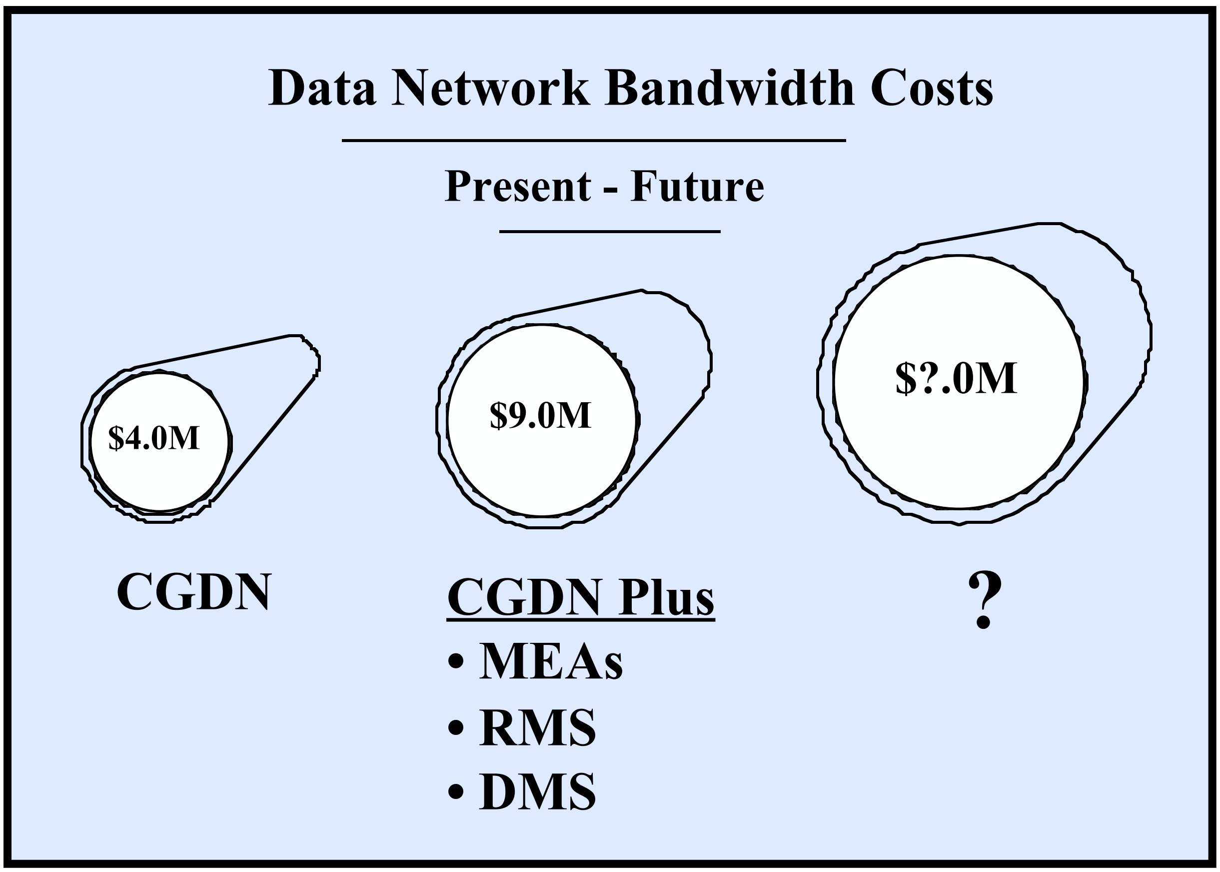


Figure 6-10: CGDN Bandwidth Costs Current and Future

6.3.2 Wireless Communications

Specialized, dual-mode cellular service (i.e., CONDOR) may be available for use in the year 2000 for global high priority clear and secure voice and data communications. This service may include administrative and operational voice communications using LEOS systems, such as Globalstar and Iridium.

Several other networking technologies, described earlier in this Chapter, are currently being used by the Coast Guard and may remain key components of the new network. These include MILSATCOM and traditional radio communications.

6.4 Criteria

Three technology areas were assessed: (1) Data Networking, (2) Mobile Communications, and (3) Requirements for Interoperability with DoD. Within these three areas, each technology, with potential for addressing current and future requirements, was carefully analyzed. Capabilities were assessed along with technology availability, cost, and ease of implementation.

DoD's DMS requirement may have considerable impact on the Coast Guard's data networking solution and was considered in network planning.

Wherever it was cost effective and possible, the network was designed to minimize single point failures and to ensure the highest reliability and survivability practical.

Figure 6-11 and Table 6-2, below, show a cost comparison of Point-to-Point and several variations of Frame Relay over a 5 year period.

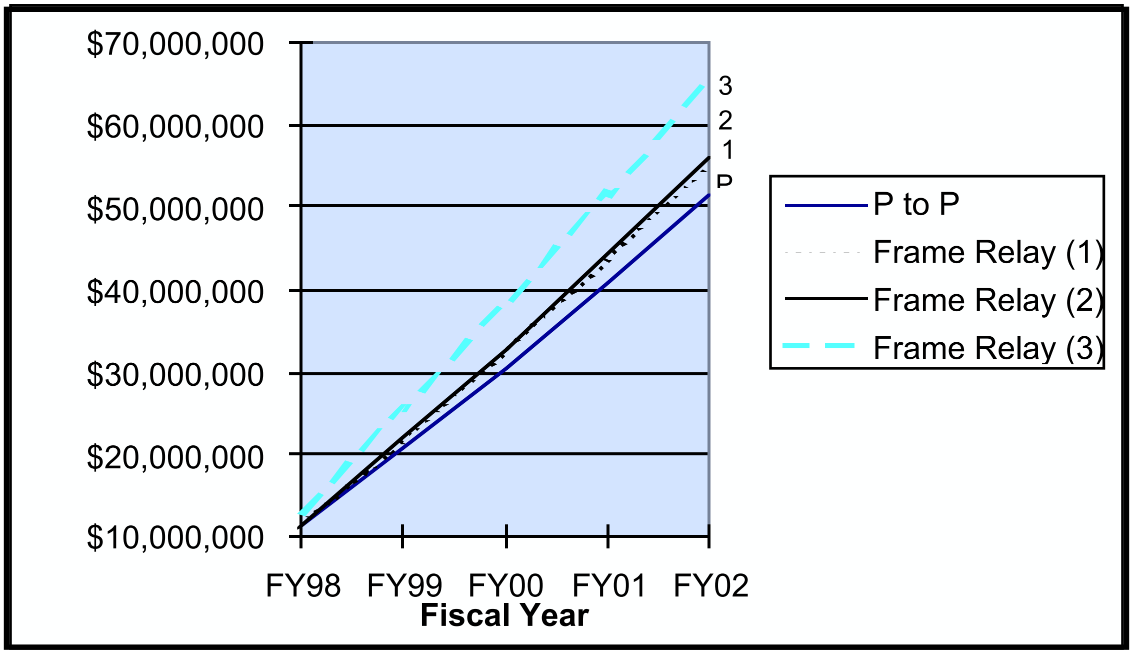


Figure 6-11: Cost Curves - T1 verses Frame Relay

Table 6-2: Bandwidth/CIR Allocations

Alternative	Bandwidth		
	TIER 1	TIER 2	TIER 3
P to P	T-1	T-1	T-1
Frame Relay (1)	T-1/384 Kbps	512 Kbps/128 Kbps	256 Kbps/128 Kbps
Frame Relay (2)	T-1/384 Kbps	512 Kbps/256 Kbps	256 Kbps/128 Kbps
Frame Relay (3)	T-1/384 Kbps	T-1/384 Kbps	256 Kbps/128 Kbps

Note: T1 = 1.544 kbps Burst Rate

384 kbps = Committed Information Rate (CIR)

From the above figure and table, it is apparent that future implementation of certain Frame Relay configurations may be more costly than Point-to-Point depending on the choice of committed information rate (CIR).

6.5 Reasoning

Capability, open systems compliance, ease of implementation, and cost were the drivers in choosing the network design. The data networking architecture for 1998 was selected because it is the most effective and capable option currently available.

Major factors considered in the selection of Point-to-Point technology for CGDN Plus:

- **Flexible and Scaleable:** Point-to-Point technology is both flexible and scaleable, and it provides the lowest technology risk and most bandwidth for the cost.

- **Open Systems Compliant:** Point-to-Point technology, using Open Shortest Path First (OSPF) routing protocol, is non-proprietary and meets government open systems requirements.

- **Speed:** T1 Point-to-Point technology will provide a significant circuit capacity improvement over the current 56 kbps backbone network and will meet all current and future Coast Guard voice, data, and video (imagery) requirements.

- **System Engineering:** Point-to-Point technology implementation requires the least up-front engineering of the available technologies. Point-to-Point overhead is roughly comparable. However, other technologies, such as SONET or ATM would require much greater amounts of engineering effort and overhead along with increase technology risk.

Additional factors to be considered:

- **Open Shortest Path First (OSPF) vs Enhanced Interior Gateway Router Protocol (EIGRP):** OSPF and EIGRP are routing protocols for use in large networks. Both of these protocols were considered for use on the new CGDN. There are several reasons why Point-to-Point technology with OSPF protocol was selected over Frame Relay with EIGRP as a networking solution. Primarily, OSPF is the open system standard router communications protocol, and any brand router can be installed on an OSPF network. EIGRP is a proprietary router communications protocol developed by CISCO Systems. This protocol is only available on routers produced by CISCO licensed manufacturers. To help reduce the difficulty in transitioning to the new and enhanced network, OSPF was selected because it requires significantly less implementation engineering than EIGRP. The INTERNET uses OSPF protocol. This presented a good example of a thoroughly tested and operational technology for Coast Guard use, since the Coast Guard is building a complex 500 node network.

If the Coast Guard should decide to use Frame Relay services in the future, major factors which may be considered in the selection of Frame Relay over Point-to-Point, at that time, may be:

- **Speed:** Frame Relay has a more granular speed capability. This means that it has the capability to have a defined Committed Information Rate (CIR), which allows a connection speed to be defined in smaller increments than Point-to-Point can provide.

- **Virtual Circuits:** Frame Relay has the capability to define Permanent Virtual Circuits (PVCs). This allows the customer to define PVCs between the various site locations (see Figure 6-12) as multiple singular circuits are installed to the Frame Relay "cloud." The "virtual" circuits allow more efficient use of the network, by providing high volume paths.

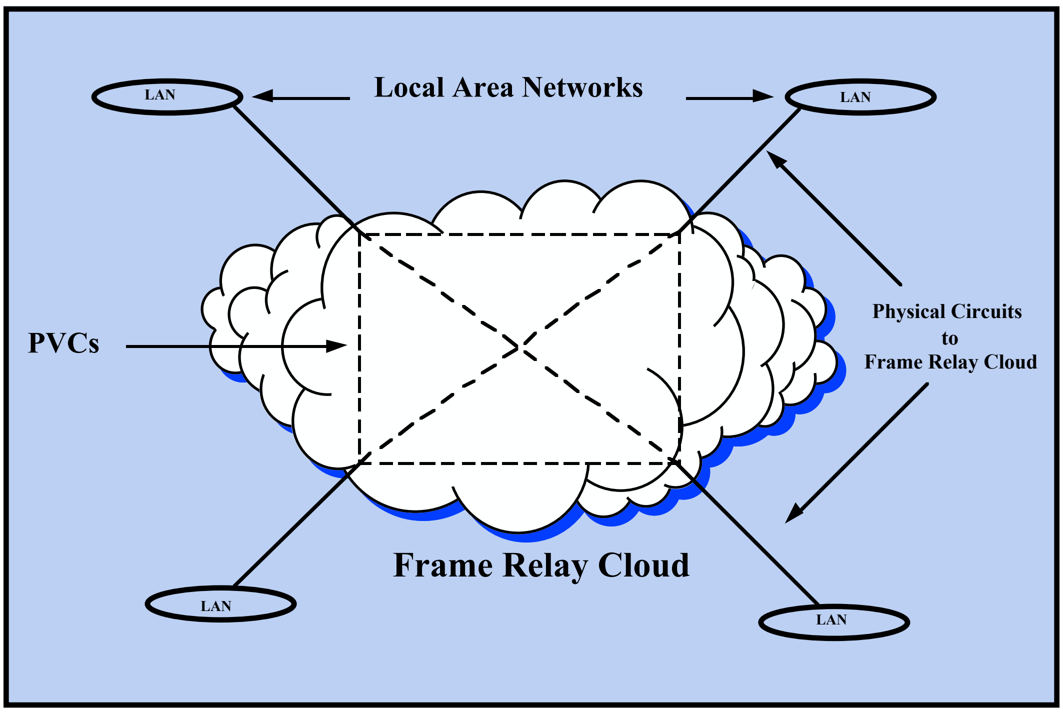


Figure 6-12: PVC Diagram

- **Cost:** In the future, Frame Relay may be less costly to install and operate than Point-to-Point. By taking advantage of the CIR capabilities, excessive and wasted bandwidth can be eliminated. After a usage history is established, the most cost effective bandwidths can be chosen, which will reduce overall costs.

- **More Flexible and Scaleable:** Due to dynamic CIR and PVC capabilities, future Frame Relay networks may be "tuned" much easier and faster than Point-to-Point. This means that the CIR can be quickly modified to provide more or less bandwidth, as required, between site locations.

6.6 Training

6.6.1 Data Network

Operator and technical training is commercially available. Classroom and computer based training courses in the latest networking technologies, such as ATM, Fast Ethernet, FDDI, Switched and Virtual LANs and WANs can be obtained from training providers, such as the Clark Technology Group or Net Guru Technologies Inc. Training may also be available from a network service provider, such as AT&T or MCI.

6.6.2 DMS

The DMS implementation plan is still incomplete and final decisions have not yet been made on training availability. The Air Force has offered to provide DMS training to all DoD organizations. However, it now appears more likely that each agency will be responsible for providing training within their own organization. Additional details, including anticipated training costs, are not yet available.

6.6.3 Military and Commercial Satellite Communications

The Coast Guard is familiar with the operational and technical aspects of several military and commercial satellite communication systems, and training in some of these areas is already in place. However, implementation of new and enhanced equipment and services may result in additional operations and technical training requirements. Training in these areas may be obtained from the service provider and/or DoD.

6.6.4 Specialized Cellular Service (CONDOR)

Training for specialized cellular service capabilities will be available from commercial service providers. For example, QUALCOM may provide CONDOR capabilities through their Globalstar LEOS system, and consequently will provide training for engineers, technicians, operators, and managers. There are currently several different courses offered at their San Diego training facility. Custom courses can also be designed and conducted at Coast Guard sites.

6.7 Recommendation

The current networking initiative, CGDN Plus, should continue, as it will provide the most capable and cost effective solution to meet Program Manager requirements. Point-to-Point connectivity, to all Coast Guard units, will provide a timely fix to an ever increasing bandwidth deficiency. The ongoing TISCOM project to implement a new data network with T1 connectivity will provide the network needed to meet all current Coast Guard data requirements.

Technology is changing at an extremely fast pace. With this in mind, the Coast Guard should consider implementing state-of-the-art technology (i.e., Frame Relay, ATM, SONET, etc.) by the year 2003, when a technology refreshment will most likely be needed. Frame Relay, for example, provides added levels of flexibility and scaleability, along with its own network management services, and may yield lower annual costs than Point-to-Point.

To provide connectivity to shore units where Frame Relay access is not available, ISDN, FTS2000 dial-up, or VSAT services could be used.

If DMS implementation comes to fruition, gateways, located at several sites, such as OSC Martinsburg and the two Areas, will provide Coast Guard shoreside access to DMS. Ships may be linked to DMS over UHF MILSATCOM which is expected to continue to be the primary means for ship-shore record message delivery. The Navy is currently committed to providing full DMS capability ashore and afloat. Coast Guard cutters (WHECs, WMECs, and possibly WPB 110s) that are frequently involved in or plan specific, significant participation in joint DoD missions will also need to follow suit. Therefore, all classes of Coast Guard cutters, from 378s down to 110s, may need to be equipped with the Navy's GBS VSAT system (tactical DMS) by the year 2003.

Gateways to the INTERNET may be located at several locations. These sites may be Headquarters, OSC Martinsburg, and an additional site on the west coast. All Coast Guard access to the INTERNET should be via these sites, where appropriate safeguards will be provided to protect Coast Guard internal systems from unauthorized access. Additional gateways at other locations may be required as INTERNET access requirements increase over time.

Regional Satellite services and INMARSAT should continue to be available with coverage of the CONUS and coastal maritime areas for shore-based and mobile Coast Guard units when needed. After which, LEOSs will greatly expand the available coverage areas by offering service everywhere on Earth, including the polar regions where current satellite services cannot reach. LEOSs will also eliminate the requirement for stabilized dish antennas on mobile platforms.

Traditional MF and HF radio communications will continue to be used primarily as a backup system for satellite equipped vessels. It will also be needed to meet certain GMDSS requirements, and to maintain Coast Guard-Navy compatibility, as the Navy plans to continue its use of traditional radio communications into the next millennium.

VHF-FM communications may be augmented or replaced by emerging technologies sometime in the distant future. However, until then, VHF-FM will continue to be used to meet NDS, GMDSS, and Coast Guard command and control requirements, as stated in Chapter 3.

Interoperability is a major benefit of specialized cellular service (CONDOR) which is expected to provide several enhancements over traditional wireless communications. Its secure (FORTEZZA card), dual mode (cellular/satellite) capability will provide mobile units with reliable world-wide voice and data connectivity. CONDOR's voice broadcast mode will provide an "all call" feature similar to the capability currently found in most traditional radio communication systems. Initial equipment and service costs will likely be high, as vendors recoup research and development costs. However, costs are expected to decline as multi-agency use of CONDOR increases.

Video requirements, for the foreseeable future, can be met using dial-up services via the PSTN. This will ensure the best possible service at the least cost to the user. PSTN dial-up services can be arranged on an “as needed” basis, which minimizes the recurring costs of leased lines.

It is important to keep in mind that costs and solutions available may vary depending on the area. For example, equipment and circuit costs in Alaska may be significantly higher than in CONUS, and the networking solutions available may be limited.

6.8 Timeline

The GANTT charts, on the following pages, show the steps that may be taken, sometime in the future, to fully implement the new Coast Guard Network-of-Networks.

Figure 6-13 shows the timeline for completion of CGDN Plus. Should the Coast Guard decide to implement new technology as a future data networking solution, Figure 13 also gives an example of an implementation schedule for Frame Relay technology across the entire CGDN.

Figure 6-14 is an estimated DMS implementation schedule, based on limited information obtained from several sources. Until DoD releases an approved project plan, a reliable time schedule will not be available.

Figure 6-15 shows an estimated schedule for implementation of several new commercial satellite technologies (i.e., regional satellite, LEOS) discussed earlier in this chapter. It also provides the schedule for an FY-99 project to replace INMARSAT-A with INMARSAT-B. INMARSAT-B provides a similar range of services to INMARSAT-A but, because it is based on modern digital telecommunications technologies, INMARSAT-B below-deck terminals are smaller and lighter. The antenna size/weight is not expected to change.

Figure 6-16 shows an implementation schedule for the Navy’s Global Broadcast System which may provide VSAT satellite receive terminals on all classes of ships. The project is in the planning stages now. GBS is expected to be available in 1998, and installed and operational by the year 2000.

Figure 6-17 shows the schedule for HFDL replacement and implementation of specialized cellular service (CONDOR) capabilities.

ID	Task Name	Start	Finish
1	**CGDN Plus Implementation**	**1/1/97**	**9/30/99**
2	Backbone Installation (Continues)	1/1/97	9/30/97
3	Tier 2 Installation	10/1/97	9/30/98
4	Tiers 3 and 4 Installation	10/1/98	9/30/99
5	CGDN Plus Implementation Complete	9/30/99	9/30/99
6			
7	**Frame Relay**	**10/1/99**	**10/1/04**
8	Backbone (begin installation)	10/1/04	10/1/04
9	Tier 2, 3, and 4 Installation Period	10/1/99	9/29/00
10	Tier 2, 3, and 4 Installation Complete	9/29/00	9/29/00
11			

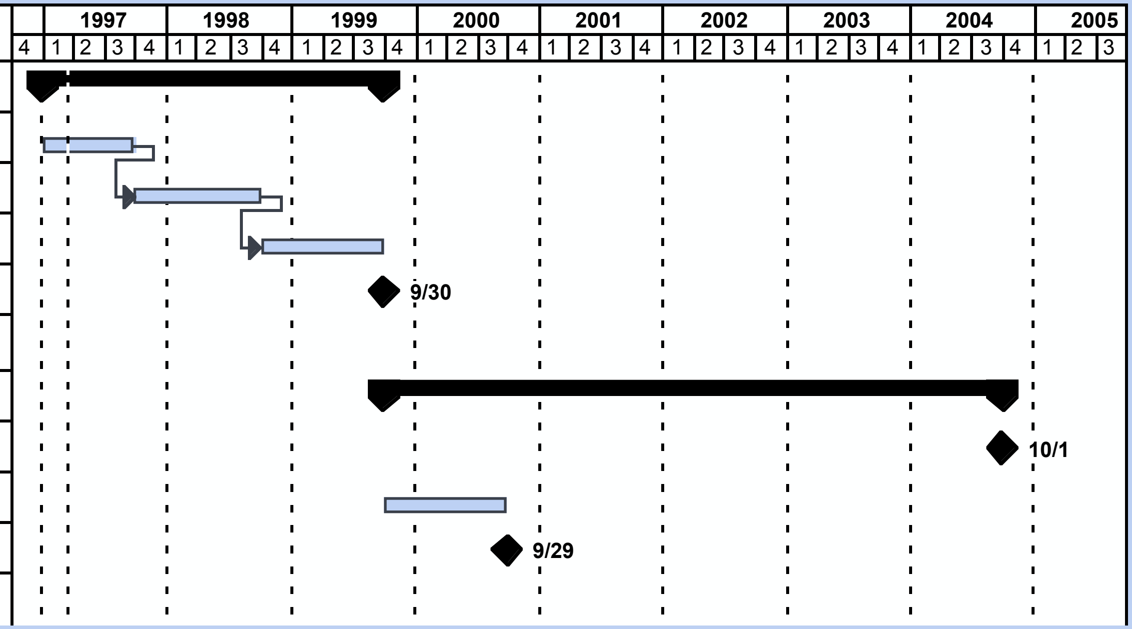


Figure 6-13: Data Network Timeline

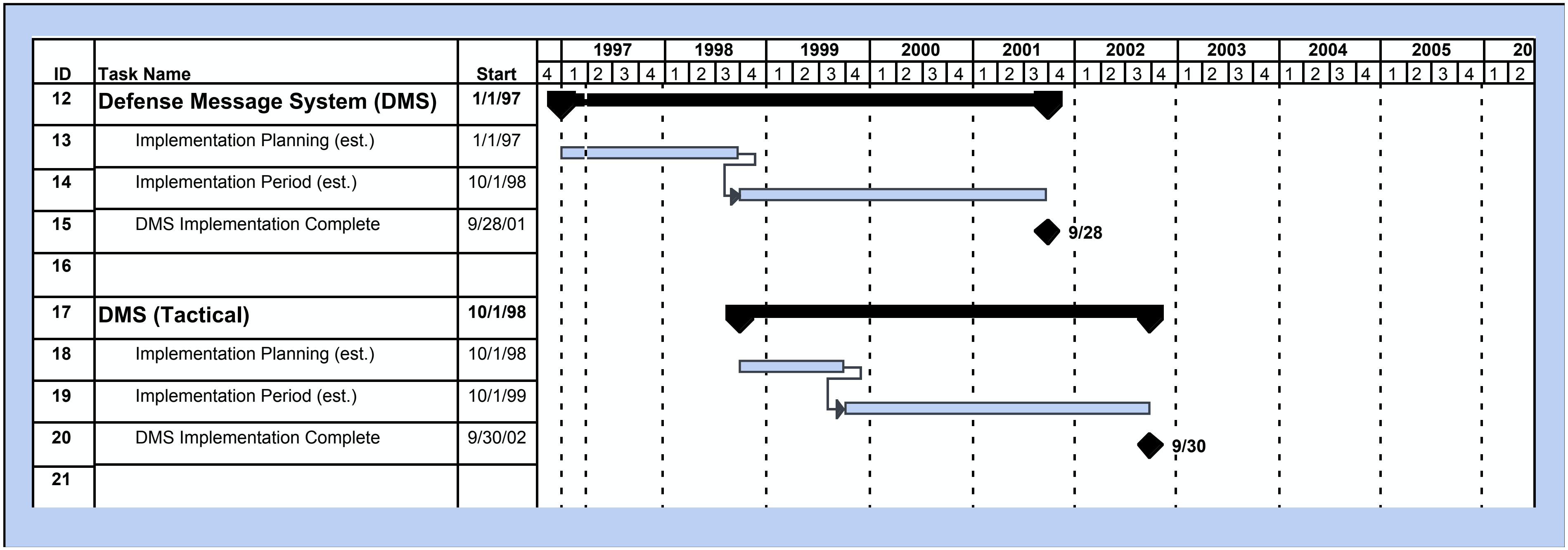


Figure 6-14: DMS Timeline

ID	Task Name	Start
22	**Commercial SATCOM**	**3/17/97**
23	**Regional**	**3/17/97**
24	RCP Submitted (HFDL Repl.)	3/17/97
25	Implementation Period	10/1/98
26	HFDL Replacement Complete	9/30/03
27	**INMARSAT A to B Replacement**	**3/17/97**
28	FY99 RCP Submitted	3/17/97
29	Implementation Period	10/1/98
30	INMARSAT Replacement Complete	9/30/03
31	**LEOS**	**3/15/01**
32	Submit FY03 RCP	3/15/01
33	Implementation Period	10/1/02
34	LEOS Implementation Complete	10/1/03
35		

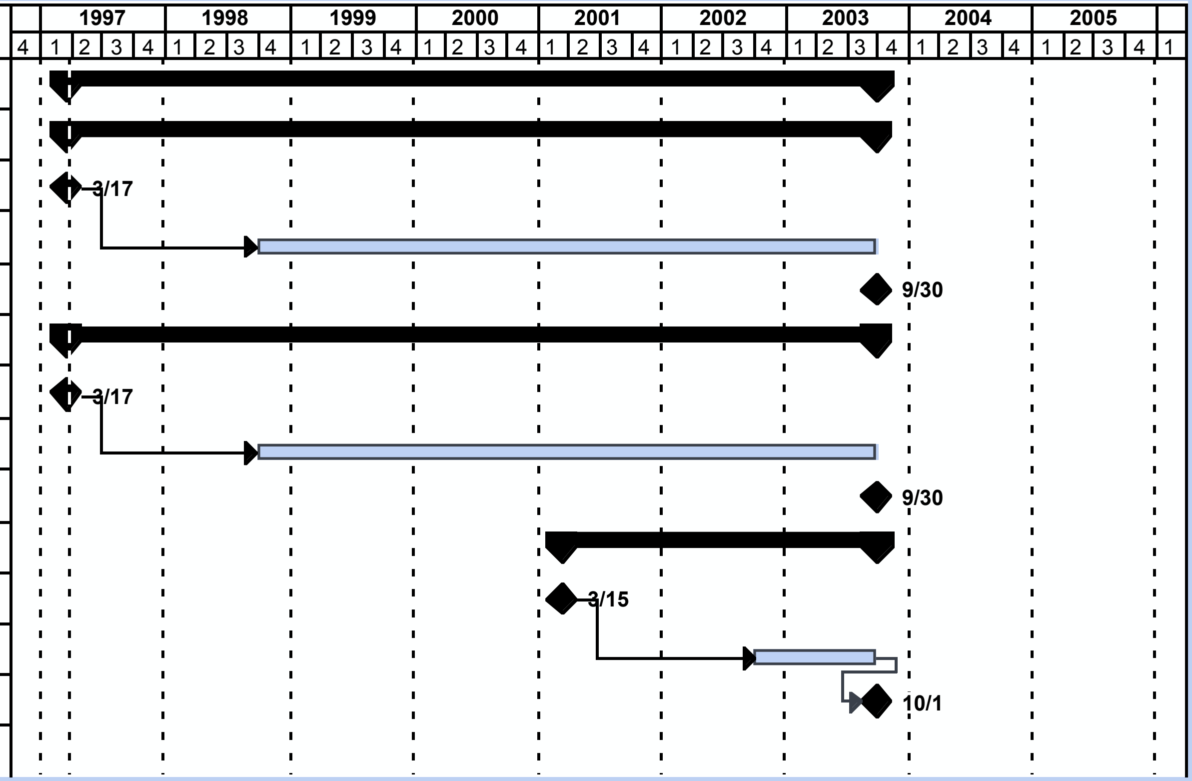


Figure 6-15: Commercial SATCOM Timeline

ID	Task Name	Start	Finish
36	**MILSATCOM**	**1/1/97**	**10/2/00**
37	**Global Broadcast System**	**1/1/97**	**10/2/00**
38	Implementation Planning	1/1/97	9/30/98
39	Implementation Period	10/1/99	9/30/00
40	GBS Implementation Complete	10/2/00	10/2/00
41			

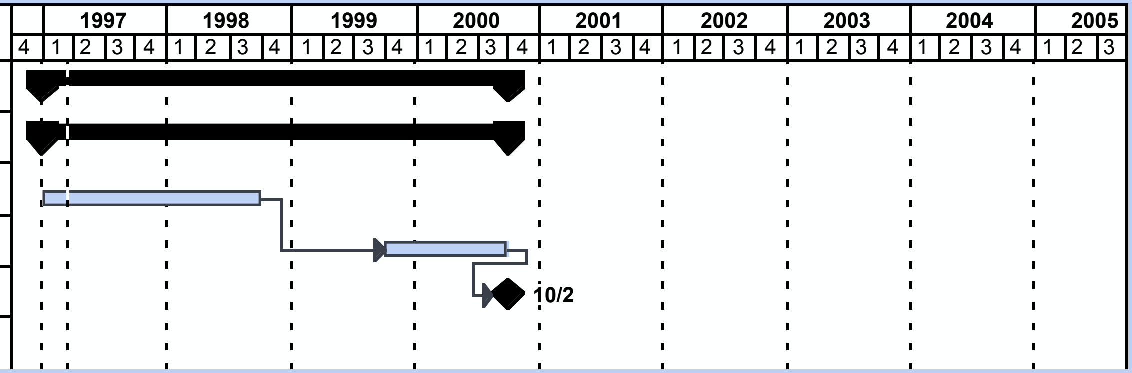


Figure 6-16: MILSATCOM Timeline

ID	Task Name	Start	Finish
42	**MF/HF Communications**	**10/1/98**	**9/30/03**
43	HFDL Phase Out Period	10/1/98	9/30/03
44			
45	**CONDOR**	**3/16/98**	**10/2/00**
46	Submit FY00 RCP	3/16/98	3/16/98
47	Implementation Period	10/1/99	9/29/00
48	Implementation Complete	10/2/00	10/2/00

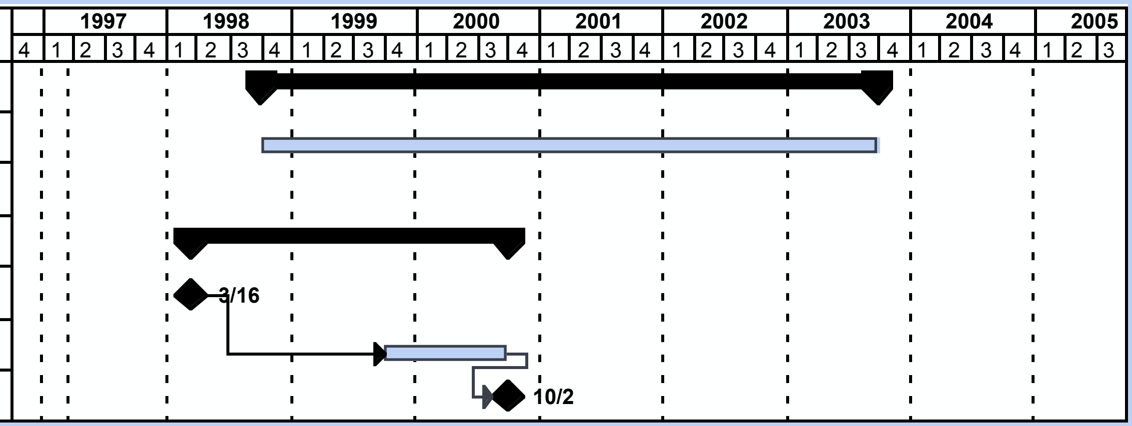


Figure 6-17: MF/HF/CONDOR Timeline

APPENDIX A
REFERENCES

- USCG C4I Baseline Architecture, dtd 14 June 1996
- USCG Communications Technology and Inter-Agency Interoperability Assessment, dtd 7 August 1996
- Command, Control and Communications Plan ANNEX KILO to LANTAREA SOP, dtd August 9, 1993
- Command, Control and Communications Plan ANNEX KILO to COMPACAREA SOP, dtd May 6, 1994
- Automatic Link Establishment Network Evaluation, Final Report
- Planning Approval for Automated Information Systems (AIS) (COMDTINST 5231.2) dtd 15 May 1988
- Systems Acquisition Manual (COMDTINST M4150.2C)
- Coast Guard Engineering Logistics Center Telecommunications Plan, dtd April 23, 1996
- Telecommunications Plan (COMDTINST M2000.4A) dtd April 20, 1988
- Telecommunications Plan (Contract No. DTCG23-91-D-TTMB12-2) dtd Feb. 5, 1993
- U.S. Coast Guard Internetworking Architecture dtd June 1993
- Appendix F - Coast Guard DMS Transition Plan dtd April 1996
- NRAD Paper “New Tactical Applications of HF Technology Hold Promise for Future Warfighters
- Commandant ltr 2070 of 26 May 1995
- OE Budget Breakdown by Fiscal Year
- ACS Customer Newsletter (Winter 1995) “The Contracting Connection”
- CCGDEIGHT 171820Z MAY 95 - Subj: Eighth District LE CommPlan
- Commandant ltr 3090 of Jan. 10, 1995, Global Command & Control System Requirements & Migration Strategy
- Commandant ltr 2070 Ser. 2380 of 16 May 94, National Distress System Coverage Analysis
- IRM Action Planning Workshop 11-13 July 1995 Results
- CCS Presentation at AFCEA Conference 23 Feb 1996
- G-T Briefing to LANTAREA Flag Conference, November 2, 1995

- Office of Command, Control and Communications (G-T) Business Plan 1996-2000
- DoD HF Remote Control System (RCS) Strategy Plan, dtd 5 Jan. 95
- National GMDSS Implementation Task Force Information Bulletin dtd 18 March 1996
- Fiscal Year 1996 Strategic Information Resource Management Plan
- Information Systems Technology Architecture (COMDTINST M5230.45A) dtd April 22 1996
- USCG Research and Development Program Long Range Plan dtd March 9, 1994
- Research, Development, Test and Evaluation (RDT&E) Appropriation Definition and Use (COMDTINST 7044.1) dtd August 10, 1994
- Office of Command, Control and Communications Strategic Plan 1993-1997 (COMDTINST M16010.7)
- Obtaining and Coordinating Research, Development, Test and Evaluation (RDT&E) Services (HQINST 5401.6)
- Finance and Procurement Concept of Operation and Strategic IRM Plan, Final Report, dtd April 15, 1994
- Naval Telecommunications Procedures Publication, NTP 4 (D)
- DMS Program Overview 1.0 (http://www.disa.mil/D2/DMS/docs/progovw/toc.html)
- ATM Wireless Networks (http://steinbrecher.com/maisonpaper.html)
- ATM Technology Initiatives in the Department of Defense (http://disa11.atd.net/atmdemo.html)
- Aviation Logistic Management Information System Analysis of Alternatives
- PMIS/JUMPS II Preliminary Technical Alternatives and Cost Analysis Report, dtd February 20, 1996
- Marine Information for Safety and Law Enforcement (MISLE) Technology Model, dtd December 4, 1996
- Fleet Logistics System (FLS) Technical Infrastructure Study (TIS) FLS TIS Requirements Analysis (Final)
- The National Information Infrastructure initiative and the Emergence of the Electronic Superhighway by Jonathan D. Blake/Lee J. Tiedrich (http://www.law.indiana.edu)
- Technology Integration Environment (http://www.les.mil/aitsjpo/tie/overview.htm)
- Navy Telemedicine Projects (http://www.matmo.org/pages/projects/navyproj.html)
- Evolution of Personal Communications by Raymond Steele (http://www.ieee.org)

- Defense Satellite Communications System (DSCS) (http://www.laafb.af.mil) (http://www.disa.mil.org/disad321.html)
- Joint Maritime Communications Strategy (JMCOMS) (http://www.spawar.navy.mil)
- Completion of the International Network (http://www.kdd.co.jp/gmm-e)
- A Demand Assigned Multiple Access (DAMA) Prototype Implementation (http://www.disa.atd.net/dama/dama.html)
- Spread Spectrum Technology (http://www.kmj.com/proxim/pxhist.html)
- Selected Topics in Communications --- Spread Spectrum Communications: Theory and Applications (http://www.eng.usf.edu)
- The Principles of Spread Spectrum Communication (http://olt.et.tudelft)
- Using Network Security Firewall Software to Improve Client and Server Security in Enterprise Networks, Technical Brief dtd July 20, 1996
- Military-Strategic/Tactical Relay (MILSTAR) System (http://www.dtic.mil)
- Formtek Journal (http://www.formtek.com/J27/Milstar.html)
- Satellite Communications Development Plan (http://www.afbmd.laafb.af.mil)
- The Bay Area Communications System (BACS), Naval Postgraduate School, dtd March 1995
- Description of Globalstar System, dtd August 10, 1995
- Commercial Satellite Communications Initiative (CSCI) (http://www.fcw.com)
- Mini-DAMA (http://www.disa.atd.net/dama)
- Challenge Athena (http://www.matmo.org.pages.projects.navyproj.html)
- Cellular Digital Packet Data (http://raleigh.ibm.com.cel.celmel.html)
- CONDOR Information: Jim Treadway at Qualcomm Inc. (616) 658-2716)
- CONDOR Information: Eric Johnson at National Security Agency (410) 684-7073

APPENDIX C
ACRONYMS AND ABBREVIATIONS

ABS	Automated Broadcast Scheduler
ACMS	Aviation Computerized Maintenance System
AMMS	Aviation Maintenance Management Information System
ADNET	Anti-Drug Network
ADNS	Automated Digital Network System
ADP	Automatic Data Processing
AIS	Automated Information System
ALE	Automatic Link Establishment
ALMIS	Aviation Logistics Management Information System
AMMIS	Aviation Maintenance Management Information System
AMPS	Advanced Mobile Phone Service
AMSC	American Mobile Satellite Corporation
AMVER	Automated Mutual Assistance Vessel Rescue System
ANDVT	Advanced Narrowband Digital Voice Terminal
ANT	Aids to Navigation Team
AOR	Area of Responsibility
AR&SC	Aircraft Repair and Supply Center
ARMS	Automated Requisition Management System
ARQ	Automatic Repeat Request
ATM	Asynchronous Transfer Mode
ATON	Aids to Navigation
ATONIS	Aids To Navigation Information System
AUTODIN	Automatic Digital Network
AUXMIS	Auxiliary Management Information System
BRI	Basic Rate Interface
C2	Command and Control
C3	Command, Control and Communications
C4I	Command, Control, Communications, Computers, and Intelligence
CAD	Computer Aided Design
CAMS	Communication Area Master Station
CASP	Computer Aided Search Program
CASREP	Casualty Report
CAW	Certificate Authority Workstations
CCGF	Commander of Coast Guard Forces
CCITT	Consultative Committee on International Telegraphy and Telephony
CDMA	Code Division Multiple Access
CDMA	Code Division Multiple Access

CDPD	Cellular Digital Packet Data
CEDS	Civil Engineering Data System
CEU	Civil Engineering Unit
CGDN	Coast Guard Data Network
CGSW	Coast Guard Standard Workstation
CGTS	Coast Guard Telecommunications System
CHCS	Composit Health Care System
CIR	Committed Information Rate
CIR	Committed Information Rate
CLAMS	Clinic Automated Management System
CMS	Communications Security Material System
COMMCEN	Communication Center
COMMSTA	Communication Station
COMSEC	Communications Security
CONDOR	Multi-mode Cellular Capability
CONUS	Continental United States
COTHEN	Customs Over the Horizon Enforcement Net
COTP	Captain of the Port
COTS	Commercial Off-The-Shelf
CP	Contingency Preparedness
CPU	Central Processing Unit
CSCI	Commercial Satellite Communications Initiative
CSN	Communication System (COMMSYS) Network
CUDIXS	Common User Digital Information Exchange Subsystem
CVS	Commercial Vessel Safety
CW	Continuous Wave (Morse Code)
DAAS	Defense Automated Addressing System
DAK	DirecPC Access Kit
DAMA	Demand Assign Multi-Access
DBS	Direct Broadcast Satellite
DCS	Defense Communications System
DDB	Distributed Database
DDD	Direct Distance Dialing
DEA	Drug Enforcement Agency
DES	Data Encryption Standard
DGPS	Differential Global Positioning System
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DLS	Digital Subscriber Line
DMR	Digital Mobile Radio
DMS	Defense Messaging System
DO	Defense Operations
DoD	Department of Defense

DOT	Department of Transportation
DSA	Director System Agents
DSC	Digital Selective Calling
DSCS	Defense Satellite Communications System
DSN	Defense Switched Network
DSP	Digital Signal Processor
DSS	Decision Support System
E-Mail	Electronic Mail
EC	Electronic Commerce
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce, and
EEZ	Exclusive Economic Zone
EHF	Extremely High Frequency
EIGRP	Enhanced Interior Gateway Router Protocol
ELT	Enforcement of Laws and Treaties
EPIRB	Emergency Position-Indicating Radio Beacons
ERO	Ethernet Router Option
FAX	Facsimile
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEC	Forward Error Correction
FINCEN	Finance Center
FLS	Fleet Logistics System
FLTSATCOM	Fleet Satellite Communications
FMIS	Facilities Management Information System
FOSC	Federal On-Scene Coordinator
FRTT	Coast Guard Fleet Broadcast (Atlantic Area)
FTP	File Transfer Protocol
FTS	Federal Telecommunications System
GBS	Global Broadcast System
GDOC	Geographic Display Operations Computer
GENSER	General Service
GFI	Government Furnished Information
GMDSS	Global Maritime Distress and Safety System
GOCC	Ground Operations Control Center
GPS	Global Positioning System
GSA	General Services Administration
GSM	Global System for Mobile Communications
HF	High Frequency
HFDL	High Frequency Data Link
HFDS	High Frequency Data System
HQ	Headquarters
HSFB	High Speed Fleet Broadcast

HTTP	HyperText Transfer Protocol
INFOSEC	Information Systems Security
INMARSAT	International Maritime Satellite
IO	Ice Operations
IP	Internet Protocol
IRM	Information Resource Management
ISB	Independent Sideband
ISDN	Integrated Services Digital Network
ITP	Integrated Terminal Program
JMCIS	Joint Maritime Command Information System
JMCOMS	Joint Maritime Communications Stragety
JSS	JMIE Support System
JUMPS	Joint Uniformed Military Pay System
kbps	Kilo Bits Per Second
kHz	kiloHertz
LAN	Local Area Network
LANT	Atlantic
LDR	Low Data Rate
LE	Law Enforcement
LEDET	Law Enforcement Detachment
LEIS	Law Enforcement Information System
LEOS	Low Earth Orbit Satellite
LMCG	Coast Guard Fleet Satellite Broadcast
LMR	Land Mobile Radio
LNM	Local Notice to Mariners
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
LSB	Lower Sideband
LUFS	Large Unit Financial System
MARDEZ	Maritime Defense Zone
Mbps	Mega Bits Per Second
MDR	Medium Data Rate
MDT	Message Distribution Terminal
MEA	Mission Essential Application
MEP	Marine Environmental Protection
MEPRS	Medical Expenses and Performance Reporting System
MF	Medium Frequency
MFI	Multi-Function Interpreter
MHS	Message Handling System
MHz	MegaHertz
MIB	Marine Information Broadcast
MILSAT	Military Satellite
MILSATCOM	Military Satellite Communications

MILSTAR	Military Strategic, Tactical, and Relay
MLA	Mail List Agent
MLC	Maintenance and Logistics Command
MLE	Maritime Law Enforcement
MPRS	Message Preparation and Review Software
MSA	Marine Science Activities
MSD	Marine Safety Detachment
MSIC	Marine Safety Information System
MSMS	Marine Safety Management System
MSN	Marine Safety Network
MSO	Marine Safety Office
MWS	Management Workstation Product
NAVCEN	Navigation Center
NAVCOMPARS	Naval Communications Processing and Routing System
NAVMACS	Naval Modular Automated Communications Sub-system
NAVNET	Navigation Network
NAVTEX	Navigational Teletype Exchange (TELEX)
NBDP	Narrow Band Direct Printing
NCC	Network Control Center
NDS	National Distress System
NIU	Network Interface Unit
NM	Nautical Miles
NOC	Network Operations Center
NPR	National Performance Review
NSA	National Security Agency
NSS	Network System Security
NTM	Notice to Mariners
OCMI	Officer in Charge of Marine Inspection
OER	Officer Evaluation Report
OGA	Other Government Agency
OIS	Operational Information System
OSA	Open Systems Architecture
OSA	Operating System Administrator
OSC	On-Scene Commander
OSC	Operations Systems Center
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OTAR	Over-the-Air Rekeying
OTAT	Over-the-Air Transfer
OTCIXS	Officer-in-Tactical Command Information Exchange Sub-system
PABX	Private Automatic Branch Exchange
PAC	Pacific
PBX	Private Branch Exchange

PC	Personal Computer
PCS	Personal Communications Services
PERSRU	Personnel Reporting Unit
PLA	Plain Language Address
PMIS	Personnel Information Management System
POC	Point of Contact
POP	Point of Presence
POP	Post Office Protocol
PORD	Preliminary Operational Requirements Document
POTS	Plain Old Telephone Service
PRI	Primary Rate Interface
PRIN	Portable RF Integrated Network
PRO	Project Resident Offices
PRTT	Coast Guard Fleet Broadcast (Pacific Area)
PSS	Port Safety and Security
PTT	Post Telephone and Telegraph
PVC	Permanent Virtual Circuits
Q&A	Question and Answer
RATT	Radio Teletype
RF	Radio Frequency
RFP	Request For Proposal
RMS	Record Message System
SAR	Search and Rescue
SARSAT	Search and Rescue Satellite System
SARTEL	Search and Rescue Telephone
SATCOM	Satellite Communications
SATRATT	Satellite Radio Teletype
SCAMP	Shipboard Computer Aided Maintenance Program
SCCB	Supply Center Curtis Bay
SCCR	Supply Center Computer Replacement
SCCS	Shipboard Command and Control System
SCI	Sensitive Compartmented Information
SCN	System Coordination Network
SDN	Secure Data Network
SHF	Super High Frequency
SIPRNET	Secret Internet Protocol Router Network
SITOR	Simplex Teletype Over Radio
SMC	SAR Mission Coordinator
SMG	Standard Mail Guard
SMTP	Simple Mail Transfer Protocol
SNS	Secure Network Server
SOCC	Satellite Operations Control Center
SOLAS	Safety Of Life At Sea

SONET	Synchronous Optical Network
SRA	Short Range Aids-to-Navigation
SSAMPS	Standard Semi-Automated Message Processing System
SSB	Single Sideband
SSMR	Shore Station Maintenance Request
STAR	Standard Automation Requisitioning
STCS	Shipboard Telecommunications Computer System
STM	Serial Tone Modem
T1	North American Carrier System (1.544 Mbps)
T3	North American Carrier System (44.736 Mbps)
TAD	Temporary Additional Duty
TCC	Transportable Communications Central
TCP	Telecommunications Plan
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TELEX	Teletypewriter Exchange Network (Western Union)
TISCOM	Telecommunications and Information Systems Command
TMMiC	Transportable Multi-Mission Communication Central
TRACEN	Training Center
TRANSEC	Transmission Security
TWX	Teletypewriter Exchange (older version of TELEX)
UFO	UHF Follow-On satellite system
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunication System
VAN	Value Added Network
VHF	Very High Frequency
VHF-FM	Very High Frequency-Frequency Modulation
VOBRA	Voice Broadcast Automation
VSAT	Very Small Aperature Terminal
VTS	Vessel Traffic Service
WAN	Wide Area Network
WAP	Wired Access Points
WWM	Waterways Management
WWMCCS	World-Wide Military Command and Control System
WWW	World-Wide Web