

NAVAL TELECOMMUNICATIONS PROCEDURES



NAVAL COMMUNICATIONS

**NTP 4 (E)**

18 JANUARY 2008

COMMANDER, NAVAL NETWORK WARFARE COMMAND  
2465 GUADALCANAL RD  
NORFOLK VA 23521-3228

DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT  
AGENCIES ONLY FOR OPERATIONAL USE, OTHER  
REQUESTS FOR THIS DOCUMENT SHALL BE REFERRED TO  
COMNAVNETWARCOM

THIS PUBLICATION CONTAINS U.S. MILITARY  
INFORMATION AND RELEASE TO OTHER THAN U.S. MILITARY  
AGENCIES WILL BE ON A NEED-TO-KNOW BASIS.

DEPARTMENT OF THE NAVY  
COMMANDER, NAVAL NETWORK WARFARE COMMAND  
2465 GUADALCANAL RD  
NORFOLK VA 23521-3228

LETTER OF PROMULGATION

1. NTP 4(E), NAVAL COMMUNICATIONS, was developed under the direction of the Commander, Naval Network Warfare Command and is promulgated for use by the U.S. Navy, Coast Guard and Marine Corps.

2. NTP 4(E) is an unclassified, non-registered publication. NTP 4(E) will remain a live document on NETWARCOM share point web site

(<http://fleetforces.navy.smil.mil/NETWARCOM/N3OPS/N35/NTP4rev/default.aspx>).


Updates will be a constant, frequent effort based on comments and feedback received from the Fleet. The concept is for this publication to always have up-to-date and accurate information. Updates and corrections to NTP 4(E) will be identified on the Record of Changes page.

3. NTP 4(E) is UNCLASSIFIED For Official Use Only (FOUO). It is **EFFECTIVE UPON RECEIPT** and supersedes NTP 4(D). It has been updated so it can better serve as the Navy's primary source of information for network and communication systems.

4. Permission is granted for authorized holders to copy or make extracts from this publication without the consent of the Commander, Naval Network Warfare Command.

5. This publication or extracts thereof may be carried in aircraft for use therein.

6. Correspondence concerning this publication should be addressed via the normal military chain-of-command to Naval Network Warfare Command, 2465 Guadalcanal Rd, Norfolk, VA 23521-3228.

  
H. D. STARLING II  
VADM, U.S. Navy  
Commander, Naval Network  
Warfare Command



## TABLE OF CONTENTS

### CHAPTER 1 - COMMUNICATION ORGANIZATION & ADMINISTRATION

- 1.1 INTRODUCTION
- 1.2 NAVAL NETWORK WARFARE COMMAND
  - 1.2.1 Naval Computer and Telecommunications Area Master Station (NCTAMS)
    - 1.2.1.1 Naval Computer and Telecommunications Station (NCTS)
    - 1.2.1.2 Navy Information Operations Command (NIOC)
  - 1.2.2 Navy Circuit Management Office (NCMO)
  - 1.2.3 Navy Marine Corps Spectrum Center (NMSC)
  - 1.2.4 Navy Communications Security Material System (NCMS)
  - 1.2.5 Navy Cyber Defense Operations Command (NCDOC)
  - 1.2.6 Naval Netwar Forcenet Enterprise (NNFE)
- 1.3 BILLETS and WATCHSTATIONS
  - 1.3.1 Communications Officer
  - 1.3.2 Radio Officer (Communications Center Officer)
  - 1.3.3 Joint Force Telecommunications Operations Center (JFTOC) Watch Officer
  - 1.3.4 Electronic Keying Material System (EKMS) Manager
  - 1.3.5 Information Assurance Manager (IAM)
  - 1.3.6 Communications Watch Officer (CWO)
  - 1.3.7 Systems Technical Control Supervisor
  - 1.3.8 Communications Center Supervisor
  - 1.3.9 Automated Data Processing Officer (ADPO)
  - 1.3.10 Systems Administrator
  - 1.3.11 Knowledge Management (KM) Process and Organization
  - 1.3.12 Information Management (IM) Process and Organization
  - 1.3.13 Staff Communications Officer
- 1.4 ADMINISTRATION
  - 1.4.1 Communications Equipment Population Summary (CEPS)
  - 1.4.2 Material Support
  - 1.4.3 Corrective Maintenance
  - 1.4.4 Inventory Control
  - 1.4.5 Communications publications
- 1.5 SAFETY
  - 1.5.1 Safety precautions
  - 1.5.2 Going aloft
  - 1.5.3 Dangerous voltages and currents
  - 1.5.4 Discharge and grounding circuits
  - 1.5.5 Adjusting electronic transmitting equipment
  - 1.5.6 Radio frequency radiation hazard
  - 1.5.7 Disposal of radioactive electronic parts
- 1.6 TRAINING AND READINESS
  - 1.6.1 General
  - 1.6.2 Training documents
  - 1.6.3 Personnel training
  - 1.6.4 NCMS assist visits (CMS A&A Team)

- 1.6.5 Communications Assistance Team (CAT)
- 1.6.6 Embarkable Staff Integration Team (ESIT)
- 1.6.7 Team Oscar
- 1.6.8 Equipment technical assist visits
- 1.6.9 Exercise and testing
  - 1.6.9.1 Command Assessment of Readiness and Training (CART)
  - 1.6.9.2 Navy Mission Essential Task (NMET)
  - 1.6.9.3 Fleet Readiness Training Plan (FRTP)
  - 1.6.9.4 Joint Task Force Exercise (JTFEX)
  - 1.6.9.5 Composite Training Unit Exercise (COMPTUEX)
  - 1.6.9.6 Deploying Group Systems Integration Testing (DGSIT)
  - 1.6.9.7 Final Integration Testing (FIT)
  - 1.6.9.8 ULTRA-C and ULTRA-S
  - 1.6.9.9 FXP 3 (CCC) drills
  - 1.6.9.10 C4I Fast Cruise

## CHAPTER 2 - AUTOMATED COMMUNICATIONS and INFORMATION SYSTEMS

### 2.1 GENERAL

### 2.2 MESSAGING SYSTEMS

- 2.2.1 DMS Overview
  - 2.2.1.1 Tactical Message Gateway (TMG)
  - 2.2.1.2 Certification Authority Workstation (CAW)
  - 2.2.1.3 Message Conversion System (MCS)
  - 2.2.1.4 DMS and Tactical DMS Proxy Afloat System
  - 2.2.1.5 Defense Message Dissemination System (DMDS)
  - 2.2.1.6 Mail List Agent (MLA)
  - 2.2.1.7 Directory System Agent (DSA)
  - 2.2.1.8 Backbone Message Transfer Agent (BMTA)
  - 2.2.1.9 Local Message Transfer Agent (LMTA)
  - 2.2.1.10 High Assurance Guard (HAG)
  - 2.2.1.11 Service Management System (SMS)
  - 2.2.1.12 Groupware Server (GWS)
- 2.2.2 Trouble Management System (TMS)
- 2.2.3 Automated Message Store and Forward (NOVA)
- 2.2.4 Personal Computer Message Terminal (PCMT)
- 2.2.5 Gateguard
- 2.2.6 Fleet Message Exchange (FMX)
- 2.2.7 Directory Update Service (DUSC)
- 2.2.8 Fleet SIPRNET Messaging (FSM)
- 2.2.9 NEWSDEALER MSS and AMHS
- 2.2.10 Naval Modular Automated Communications Subsystem (NAVMACS)
- 2.2.11 Common User Digital Information Exchange Subsystem (CUDIXS)
- 2.2.12 Submarine Satellite Information Exchange Subsystem (SSIXS)
- 2.2.13 Battle Group Information Exchange Subsystem (BGIXS)
- 2.2.14 Navy Regional Enterprise Message System (NREMS)

- 2.3 FLEET BROADCAST
  - 2.3.1 GENERAL INFORMATION
  - 2.3.2 Control of the Fleet Broadcasts
  - 2.3.3 Communications Guard
  - 2.3.4 Broadcast Identification
  - 2.3.5 Frequencies
  - 2.3.6 Circuit configuration
  - 2.3.7 Cryptographic coverage
  - 2.3.8 Broadcast message numbering
  - 2.3.9 Broadcast message format
  - 2.3.10 Broadcast recaps
  - 2.3.11 Broadcast service messages
  - 2.3.12 Broadcast off the air monitoring (OTAM)
  
- 2.4 TYPES OF BROADCASTS
  - 2.4.1 Fleet Multichannel Broadcast System
  - 2.4.2 World-wide TACAMO (WTAC)
  - 2.4.3 USW Patrol (VP) broadcast
  - 2.4.4 SCI Fleet broadcasts
  
- 2.5 MANAGEMENT AND CONTROL SYSTEMS
  - 2.5.1 Automated Digital Networking System (ADNS)
  - 2.5.2 Radio Communications System (RCS)
  - 2.5.3 Navy Orderwire (NOW)
  - 2.5.4 Automated Network Control Center/Automated Technical Control (ANCC/ATC)
  - 2.5.5 Multi-circuit patch panel (MCP)
  - 2.5.6 SA 2112 (V) SAS
  - 2.5.7 Timeplex LINK 2+
  
- 2.6 NETWORK SERVICES AND ARCHITECTURE
  - 2.6.1 Routing Architecture
  - 2.6.2 DISN transport services
  - 2.6.3 Communications within DISN Data Services Networks
  - 2.6.4 Switches and Routers
  - 2.6.5 Unclassified but Sensitive Internet Protocol Network (NIPRNET)
  - 2.6.6 Secret Internet Protocol Network (SIPRNET)
  - 2.6.7 Authorized Service Interruption (ASI)
  - 2.6.8 Carrier Rates (T1, E1, OC3, OC12, etc)
  
  - 2.6.9 IT-21
    - 2.6.9.1 Integrated Shipboard Networking System (ISNS)
    - 2.6.9.2 Navy Tactical Command Support System (NTCSS)
  
    - 2.6.9.3 Fleet Network Operations Center (FLTNOC)
      - 2.6.9.3.1 INCHOP/OUTCHOP
      - 2.6.9.3.2 IT21 FLTNOC Security
      - 2.6.9.3.3 Customers and Support
      - 2.6.9.3.4 Navy Regional Networks Operations and Security Center (NAVRNOSC)

- 2.6.9.3.5 Program Executive Office, Command, Control,  
Communications, Computers and Intelligence (PEO C4I)
- 2.6.10 Navy Marine Corps Intranet (NMCI)
- 2.6.11 Overseas Navy Enterprise Network (OneNet)
- 2.6.12 Consolidated Afloat Networks and Enterprise Services  
(CANES)
- 2.6.13 Global Information Grid - Bandwidth Expansion (GIG-BE)
- 2.6.14 High Speed Global Ring (HSGR)
  - 2.6.14.1 HSGR advantages
  - 2.6.14.2 HSGR Network Management
- 2.6.15 N2N - NOC to NOC
  - 2.6.15.1 N2N remote restoration
  - 2.6.15.2 N2N Security
  - 2.6.15.3 Failure of the DISN services at the IT-21 FLTNOG  
(failover)
- 2.6.16 Classified Trusted Network Protect Policy (CTNPP)/  
Unclassified Trusted Network Protect Policy (UTNPP)
- 2.6.17 IP Version (IPv6)
- 2.6.18 Global Command and Control System - Maritime (GCCS-M)
  
- 2.7 VOICE AND VIDEO SERVICES
  - 2.7.1 Voice over IP (VoIP)
  - 2.7.2 DoD Video Teleconferencing (VTC) Service
  - 2.7.3 Defense Switched Network (DSN)
  - 2.7.4 Defense Red Switched Network (DRSN)
  - 2.7.5 Integrated Services Digital Network (ISDN)
  - 2.7.6 Plain Old Telephone System (POTS)
  - 2.7.7 Afloat Personnel Telecommunications Systems (APTS)
  - 2.7.8 KY68 Digital Subscriber Voice Terminal (FDVT)
  - 2.7.9 Video Information Exchange System (VIXS)
  - 2.7.10 DISN Video Service Global (DVSG)
  - 2.7.11 STU / STE (Secure telephone)
  - 2.7.12 Advanced Narrowband Digital Voice Terminal (ANDVT)
  - 2.7.13 Future Narrowband Data Terminal (FNBBDT) standard
  
- 2.8 INTELLIGENCE AND CRYPTOLOGIC SYSTEMS
  - 2.8.1 Joint Services Processing Systems (JSIPS-N)  
Concentrator Architecture (JCA)
  - 2.8.2 Global Command and Control System - Integrated  
intelligence and imagery
  - 2.8.3 Joint Deployable Intelligence Support System (JDISS)
  - 2.8.4 Tactical exploitation system - Navy
  - 2.8.5 Integrated Broadcast System (IBS)
  - 2.8.6 Radiant Mercury
  - 2.8.7 Sensitive Compartmented Information (SCI) networks

- 2.8.8 Joint Worldwide Intelligence Communications System (JWICS)

### CHAPTER 3 - MESSAGE PROCESSING PROCEDURES

- 3.1 INCOMING MESSAGE HANDLING
  - 3.1.1 General
  - 3.1.2 Reception and duplication checking
  - 3.1.3 Precedence
  - 3.1.4 Internal distribution
- 3.2 OUTGOING MESSAGE HANDLING
  - 3.2.1 General
  - 3.2.2 Message release authority
  - 3.2.3 Message completeness and accuracy
  - 3.2.4 Circuit selection and delivery
  - 3.2.5 Transmission of classified messages under emergency conditions
  - 3.2.6 Message cancellation
  - 3.2.7 Transmission of U.S classified traffic to allied nations
  - 3.2.8 Transmission Release Code (TRC)
  - 3.2.9 Special Handling Designations (SHD)
- 3.3 SERVICE ACTION
  - 3.3.1 General
  - 3.3.2 Operating Signals (OPSIG)
  - 3.3.3 Prosigns and passwords
  - 3.3.4 Tracer action
  - 3.3.5 Message corrections and cancellations
- 3.4 MESSAGES REQUIRING SPECIAL HANDLING
  - 3.4.1 General
  - 3.4.2 Special Category (SPECAT) messages - general
  - 3.4.3 Special category (SPECAT) SIOP-ESI
  - 3.4.4 Special Category (SPECAT) Exclusive For
  - 3.4.5 Tight Control (TICON)
  - 3.4.6 Emergency Action Messages (EAM)
  - 3.4.7 White Pinnacle (EA CELL) message injects
  - 3.4.8 Limited Distribution (LIMDIS)
  - 3.4.9 American Red Cross (AMCROSS) messages
  - 3.4.10 Top Secret
  - 3.4.11 Personal For
- 3.5 MESSAGE FORMATS
  - 3.5.1 General
  - 3.5.2 Originating Station Routing Indicator (OSRI)
  - 3.5.3 Station Serial Number (SSN)
  - 3.5.4 Routing
  - 3.5.5 ACP 128
  - 3.5.6 Modified ACP 126
  - 3.5.7 ACP 127
  - 3.5.8 ACP 126



- 3.5.9 Defense Special Security Communications Systems (DSSCS)
  - 3.5.9.1 DSSCS Plain Language Addresses and Routing Indicators
  - 3.5.9.2 Legacy Address Directory Service (LADS)
  - 3.5.9.3 Classification of messages (Transmission Control Codes)
  - 3.5.9.4 CRITIC Message Processing
    - 3.5.9.4.1 Transmission
    - 3.5.9.4.2 CRITIC Message Format
    - 3.5.9.4.3 CRITIC Acknowledgement - Relay Stations
    - 3.5.9.4.4 CRITIC Handling Procedures - Relay Stations
- 3.5.10 Joint Message Preparation System (JMPS)
- 3.5.11 Common Message Processing (CMP) application

### 3.6 LOGS AND FILES

- 3.6.1 General
- 3.6.2 Master Station Log (MSL)
- 3.6.3 Central message log
- 3.6.4 Top Secret control log
- 3.6.5 Circuit logs
- 3.6.6 Broadcast circuit number log and record destruction
- 3.6.7 Message files
- 3.6.8 File maintenance
- 3.6.9 Embarked command files
- 3.6.10 Communications center master file
- 3.6.11 Crypto center file
- 3.6.12 Broadcast files
- 3.6.13 Records disposal

## CHAPTER 4 - COMMUNICATIONS SECURITY

- 4.1 General
- 4.2 COMSEC incident
- 4.3 COMSEC insecurity
- 4.4 Crypto markings
- 4.5 COMSEC material
- 4.6 Watch-to-Watch Inventory
- 4.7 Clearance requirements
- 4.8 Access to NATO information
- 4.9 Crypto access
  - 4.9.1 Two Person Integrity (TPI)
- 4.10 Access to classified communications spaces
- 4.11 Access and visitor control
- 4.12 Safe combinations
- 4.13 Classified storage
- 4.14 Beadwindow
- 4.15 Routine destruction procedures
- 4.16 Emergency destruction
- 4.17 Electronic spillages
- 4.18 Operations Security (OPSEC)

- 4.19 TEMPEST
- 4.20 EKMS training visits and inspections

## CHAPTER 5 - SHIP / SHORE AND SHIP / SHIP COMMUNICATIONS

- 5.1. INTRODUCTION
  - 5.1.1 World coverage
  - 5.1.2 Current regional area of responsibility capabilities
  - 5.1.3 Problem areas
  - 5.1.4 Unauthorized transmissions
  - 5.1.5 Violation reports
  - 5.1.6 Harmful interference - Communications jamming, imitative  
Communications deception
  - 5.1.7 Coast Guard HF ship/shore circuits
  - 5.1.8 HF Internet Protocol (HF-IP)
  - 5.1.9 Afloat Electromagnetic Spectrum Operations (AESOP)
  - 5.1.10 Frequency management
  - 5.1.11 Frequency restrictions and various theater of operation
- 5.2 SATELLITE COMMUNICATIONS
  - 5.2.1 General
  - 5.2.2 Ultra-high frequency (UHF) Satellite Communications
  - 5.2.3 Super-high frequency (SHF) defense Satellite Communications Systems (DSCS)
  - 5.2.4 Commercial Wideband Satellite Communications Program (CWSP)
  - 5.2.5 Commercial Broadband Satellite Program (CBSP)
  - 5.2.6 Wideband Gapfiller System (WGS)
  - 5.2.7 Navy Extremely High Frequency (EHF) Satellite program
    - 5.2.7.1 MILSTAR
    - 5.2.7.2 Interim Polar System (IPS)
    - 5.2.7.3 EHF Time Division Multiple Access (TDMA) Interface (TIP)
    - 5.2.7.4 EHF Systems Services
    - 5.2.7.5 Obtaining EHF Satellite Access
    - 5.2.7.6 After Action Report (AAR)
    - 5.2.8 Mobile subscriber service (Iridium)
    - 5.2.9 INMARSAT High speed data
    - 5.2.10 Global Broadcast System (GBS)
    - 5.2.11 Television Direct to Sailor (TV-DTS)
    - 5.2.12 DoD gateways
    - 5.2.13 DoD Teleport
    - 5.2.14 JMINI (Joint (UHF) MILSATCOM Network Integrated Control System )) /DAMA SAC II
- 5.3 SUBMARINE COMMUNICATIONS
  - 5.3.1 Broadcast Control Authority (BCA)
  - 5.3.2 Base Consolidated Telecommunications Center (BCT)
  - 5.3.3 Submarine broadcast system
  - 5.3.4 VLF Digital Information Network (VERDIN) broadcast
  - 5.3.5 VLF/LF SI VLF Secure, NATO VALLOR, SI VALLOR circuits
  - 5.3.6 Information Screening and Delivery System (ISDS)
  - 5.3.7 Warrior Pull

- 5.3.8 HF VALLOR circuit
- 5.3.9 IP Communications

## CHAPTER 6 - BASIC COMMUNICATIONS

- 6.1 General
- 6.2 Ship/Shore circuit modes of operation
- 6.3 Full period termination
  - 6.3.1 Full period termination reports
  - 6.3.2 Circuit activation
  - 6.3.3 Maintaining a full period termination
  - 6.3.4 Message continuity
  - 6.3.5 Loss of termination (shore)
  - 6.3.6 Termination shifts
  - 6.3.7 Termination continuity
- 6.4 Primary ship/shore circuits
  - 6.4.1 Ship call-up for primary ship/shore (Duplex mode)
  - 6.4.2 Shore station response (Duplex Mode)
  - 6.4.3 Ship call-up (Half-Duplex)
  - 6.4.4 Shore station response (Half-Duplex)
  - 6.4.5 Ship call-up (Simplex mode)
  - 6.4.6 Shore station response (Simplex mode)
- 6.5 Automated merchant vessel reporting (AMVER)
- 6.6 Net Control Station (NECOS)
- 6.7 Free Net
- 6.8 Directed Net
- 6.9 Alternate Net Control Station (ALTNECOS)
- 6.10 Status boards
- 6.11 Logging out a circuit
- 6.12 Emission Control (EMCON)
- 6.13 Operational Shipboard circuits
- 6.14 UHF AUTOCAT/SATCAT middleman relay procedures
- 6.15 Non-electronic relay systems
- 6.16 High Frequency - Automatic Link Establishment (HF-ALE)
- 6.17 Very high Frequency and Ultra High Frequency Line-of-Sight (LOS) Communications
- 6.18 Digital Wideband Transmission System (DWTS)
- 6.19 Tactical Switching System (TSS)
- 6.20 Enhanced position location reporting system - Data radio (EPLRS-DR)
- 6.21 High Frequency (HF)
- 6.22 Very Low Frequency (VLF)
- 6.23 Very High Frequency (VHF)
- 6.24 Bandwidth management
- 6.25 Communications Control Ship (CCS)

## CHAPTER 7 - ALLIED/COALITION COMMUNICATIONS

- 7.1 CENTRIXS - Maritime
  - 7.1.1 NETWARCOM C4 TYCOM
  - 7.1.2 PRNOC CENTRIXS Services

- 7.1.3 UARNOC CENTRIXS Services
- 7.1.4 IORNOC CENTRIXS Services
- 7.1.5 CENTRIXS In-Service Engineering Agent (ISEA)
- 7.1.6 CENTRIXS Central Design Agent (CDA)
- 7.1.7 CENTRIXS User
- 7.1.8 Afloat CENTRIXS User
- 7.1.9 Shore CENTRIXS User Access
- 7.1.10 CENTRIXS IA/CND Responsibilities
- 7.1.11 CENTRIXS/CAS Help Desk Responsibilities
  
- 7.2 Global CENTRIXS Network
  - 7.2.1 CENTRIXS Enclaves
  - 7.2.2 CENTRIXS Four Eyes (CFE)
  - 7.2.3 Global Counter-Terrorism Task Force (GCTF)
  - 7.2.4 Multi-Coalition Force Iraq (MCFI)
  - 7.2.5 GCTF Communities of Interest (COI)
  - 7.2.6 Combined Naval Forces CENTCOM (CNFC)
  - 7.2.7 Cooperative Maritime Forces Pacific (CMFP)
  - 7.2.8 Bilateral Networks
  - 7.2.9 CENTRIXS-Korea (CENTRIXS-K)
  - 7.2.10 CENTRIXS-Japan (CENTRIXS-J)
  
- 7.3 NATO Initial Data Transfer System (NIDTS)
  - 7.3.1 NIDTS connection requirements
  
- 7.4 Battle Force Electronic Mail 66 (BFEM)
  - 7.4.1 BFEM Configuration
  - 7.4.2 BFEM Technical support
  
- 7.5 Common SIPRNET Domain (CSD)
  
- 7.6 GIRFFIN
  - 7.6.1 GRIFFIN Account Setup
  
- 7.7 High Frequency Internet Protocol (HFIP) Networking with coalition partners
- 7.8 UHF LOS Subnet Relay (SNR) with Coalition Partners / Line of Sight and Beyond Line of Sight Networking with Coalition Partners
- 7.9 High Frequency Internet Protocol and Subnet Relay (HFIP /SNR)
- 7.10 AUSCANNZUKUS Background

## **CHAPTER 8 - COLLABORATIVE TOOLS**

- 8.1 Collaboration at Sea (CAS)
  - 8.1.2 IBM SAMETIME
  - 8.1.3 Persistent Chat (PCHAT)
  
- 8.2 Task Force Web/Navy Enterprise Portal
- 8.3 Intra-Amphibious Ready Group Distributive Collaboration planning (IDCP)
- 8.4 Defense Collaborative Tool Suite (DCTS)

**CHAPTER 9 - VOICE COMMUNICATIONS**

- 9.1 General
- 9.2 Frequencies
- 9.3 Call Signs
- 9.4 Kick Procedures
- 9.5 Voice Logs
- 9.6 Secure Voice Communications

**CHAPTER 10 - COMMERCIAL COMMUNICATIONS AT SEA**

- 10.1 SHIPCOM (AT&T)

**CHAPTER 11 - INFORMATION ASSURANCE/COMPUTER NETWORK DEFENSE**

- 11.1 Information Assurance (IA)
  - 11.1.1 Information Assurance Reporting
  - 11.1.2 Malicious Code and Viruses
  - 11.1.3 Anti-Virus Software
  - 11.1.4 Guarding your PC against Viruses
  - 11.1.5 Keeping your PC Virus Free
- 11.2 Computer Network Defense
- 11.3 Incident Handling Reports
- 11.4 Basic Incident Handling Guidelines
- 11.5 INFOCON
- 11.6 Red Team Surveys
- 11.7 Computer Tasking Orders (CTO)
- 11.8 Public Key Infrastructure (PKI)

## APPENDICES

APPENDIX A - List of Acronyms and abbreviations

APPENDIX B - COMSPOT reporting

APPENDIX C - Content Indicator Codes (CICs) for use with Navy Legacy messaging systems

APPENDIX D - Communications Information Bulletins and Advisories (CIB/CIA)

APPENDIX E - Frequency emission, bands, and designators

APPENDIX F - Military Affiliated Radio System (MARS)

APPENDIX G - Visual Communications

APPENDIX H - Communications instructions and procedures for Naval activities communicating with US Flag merchant ships (MERSHIPS)

APPENDIX I - Sample drill packages

- Standard PRE-EX C4I Drill (Sample) Package Alpha (UHF SECURE/NON-SECURE)
- Standard PRE-EX C4I Drill (Sample) Package Bravo (HF SECURE/NON-SECURE)
- Standard PRE-EX C4I Drill (Sample) Package Charlie (EHF Performance and Circuit activation)
- Standard PRE-EX C4I Drill (Sample) Package Charlie one (EHF Point-to-Point)
- Standard PRE-EX C4I Drill (Sample) Package Delta (Battle Force E-mail Activation)
- Standard PRE-EX C4I Drill (Sample) Package Echo (Warfare Commanders/Frequency shift and kicks)
- Standard PRE-EX C4I Drill (Sample) Package Echo one (Primary guarded 24 Hour roll calls)
- Standard PRE-EX C4I Drill (Sample) Golf Package Foxtrot (ATO and DIMS Transmission (various) paths )
- Standard PRE-EX C4I Drill (Sample) Package Golf (VTC Activation)
- Standard PRE-EX C4I Drill (Sample) Package Hotel (HF TTY Activation)
- Standard PRE-EX C4I Drill (Sample) Package India (OTAT/OTAR Activation)
- Standard PRE-EX C4I Drill (Sample) Package Juliet (Restore UHF DAMA)
- Standard PRE-EX C4I Drill (Sample) Package Kilo (Activate and Initiate demand call Via KY-68)
- Standard PRE-EX C4I Drill (Sample) Package Lima (CSG/ESG/Bandwidth Management)

- Standard PRE-EX C4I Drill (Sample) Package Mike (CENTRIXS replication/cross domain solution)
- Standard PRE-EX C4I Drill (Sample) Package November (Communicate via CENTRIXS email)
- Standard PRE-EX C4I Drill (Sample) Package Oscar (River City)
- Standard PRE-EX C4I Drill (Sample) Package Papa (INFOCON Exercise)
- Standard PRE-EX C4I Drill (Sample) Package Quebec (CND Incident Assurance monitoring)
- Standard PRE-EX C4I Drill (Sample) Package Romeo (Information Assurance Monitoring )
- Standard PRE-EX C4I Drill (Sample) Package Sierra (GBS)
- Standard PRE-EX C4I Drill (Sample) Package Tango (C4I Jeopardy PUBEX)

**LIST FIGURES**

- 1-1 NNFE Organization
- 1-2 NNFE Functions
  
- 2-1 Message Traffic Process
- 2-2 NOVA Configuration
- 2-3 FMX/DUSC Configuration
- 2-4 NAVMACS II Configuration
- 2-5 CUDIXS Capabilities
- 2-6 ISNS Architecture
- 2-7 NOC Core Equipment
- 2-8 IT21 FLTNOG Architecture
- 2-9 CANES CCE Infrastructure
- 2-10 High Speed Global Ring Architecture
- 2-11 High Speed Global Ring Mesh Topology
- 2-12 HSGR to FLTNOG Entry Points
- 2-13 DISN failure to UARNOC
- 2-14 Secure Voice Equipment
- 2-15 CIPHERTAC 2000 (CTAC)
- 2-16 Radiant Mercury
  
- 3-1 Common Message Format Lines
- 3-2 Send and Receive Log
- 3-3 Broadcast Circuit Number Log
  
- 4-1 BEADWINDOW Codes
  
- 5-1 HFIP/SNR Architecture
- 5-2 UFO Satellite Constellations
- 5-3 CWSP Architecture
- 5-4 CWSP Satellite Coverage
- 5-5 WGS Coverage
- 5-6 Milstar EHF Constellations
- 5-7 UFO EHF Constellations
- 5-8 Approximate polar EHF Coverage (2 satellites)
- 5-9 Approximate EC Spot Beam Coverage
- 5-10 Iridium ground architecture
- 5-11 Iridium Space Segment
- 5-12 INMARSAT Constellations
- 5-13 Conceptual GBS Architecture
- 5-14 GBS Concept of Operations Overview
- 5-15 Sample/Generic UFO/G Beam Coverage
- 5-16 UFO GBS Payload Configuration
- 5-17 Example UFO/G Configuration A
- 5-18 GBS UFO/G Phase 2 Coverage w/ Sample Beam Locations
- 5-19 DoD Gateway Locations
- 5-20 STEP Site Locations
- 5-21 DoD Teleport Architecture
- 5-22 DAMA SAC & JMINI IOC Control System Architecture
- 5-23 LF/VLF Fixed Submarine Broadcast Architecture
- 5-24 Current Submarine IP Architecture
- 5-25 Future Submarine IP Architecture



- 6-1 DWTS
- 6-2 SINCGARS Concept of Operation
  
- 7-1 CENTRIXS-M Organizational Relationships
- 7-2 CENTRIXS-M Global Connections
- 7-3 Current CENTRIXS Architecture (Single NOC)
- 7-4 NIDTS basic Architecture
- 7-5 Common SIPRNET Domain
- 7-6 HFIP and SNR OV-1
- 7-7 SNR System View
- 7-8 CENTRIXS LOS/ELOS Routing Architecture
- 7-9 AUSCANNZUKUS Interoperability Focus
  
- 9-1 Kick Procedure Example

**LIST OF TABLES**

- 1-1 NCTAMS Operational Organization
- 2-1 TACTERM Equipment
- 5-1 UFO Capabilities
- 5-2 U.S. Navy EHF Terminals
- 5-3 Milstar I LDR Channel-to-Beam Assignments
- 5-4 Milstar II MDR Channel-to-Beam Assignments
- 6-1 Transmitter/frequency Status Terminology
- 7-1 CAPCO Classification Markings
- 7-2 User Information

## PREFACE

The focus of NTP-4 Echo (Naval Communications) is to provide a basic manual addressing C4I concepts and capabilities in the U.S. Navy. Due to increased proliferation of Information Technology (IT) within DoN and the high demand for information dominance within the battle space, the need for a "primary source" C4I document has never been greater. To that end, Naval Network Warfare Command initiated a major revision to this publication reflecting the latest C4I equipment/systems in use today. This document was developed through a collaborative effort with Fleet, Numbered Fleet, Type Commanders, and other components of the Naval Netwar Forcenet Enterprise (NNFE) and serves to meet the following objectives:

1. Outline Navy communications shore/afloat organization.
2. Identify automated systems ashore and afloat to support Navy messaging.
3. Provide guidance for message processing procedures.
4. Identify Communications Security (COMSEC) measures and controls.
5. Identify satellite communications capabilities, systems, and equipment.
6. Identify submarine communications capabilities, systems, and equipment.
7. Outline Navy communications ship/shore circuit modes of operation.
8. Identify Allied/coalition communications capabilities, systems, and equipment.
9. Identify collaboration tools for use on Navy/Joint enterprise networks.
10. Provide guidance for operating and defending afloat and shore network communications systems (to include Information Assurance Vulnerability Management (IAVM) and computer incident reporting).
11. Provide guidance for Communications Spot (COMSPOT) reporting.
12. Provide sample C4I drill packages (used in conjunction with FXP-3).

To further this collaborative effort, NETWARCOM has made NTP 4 Echo available on the NETWARCOM Enterprise Workspace (NEWS) SIPRNET website at:

<http://www.fleetforces.navy.smil.mil/netwarcom/n3ops/n35/ntp4ref/default.axps>. A blog has been set up on the right hand side of this webpage to allow for continuous feedback from the Fleet on recommended changes, additions and deletions. Comments will be consolidated and adjudicated monthly before presentation to the Primary Review Authority (PRA) for approval. NETWARCOM will then announce approved changes via a Navy Telecommunications Directive.

All users of Navy C4I equipment and systems are encouraged to assist NETWARCOM in continuing to improve the value and relevance of this publication.

## CHAPTER 1

### COMMUNICATIONS ORGANIZATION AND ADMINISTRATION

#### 1.1 INTRODUCTION

This chapter provides a complete description of the Naval Network Warfare Command composition and the Naval NETWAR FORCEnet Enterprise (NNFE) as well as associated Shore and Fleet components required to achieve warfare mission areas in Navy C4I. Additionally, it provides guidance concerning basic communications safety and an overview of communications training.

#### 1.2 NAVAL NETWORK WARFARE COMMAND (NETWARCOM)

NETWARCOM is the Navy's central operational authority for Command, Control, Communications, Computers and Intelligence (C4I), Space, and Information Operations (IO) in support of Naval forces afloat and ashore. Established in July of 2002, NETWARCOM is unique in that it is the Navy's only Capability TYCOM for C4I. In 2004, NETWARCOM was designated as Director, C4I and Modernization (USFF N6) and in 2005 assumed responsibility for the Navy COMSEC Management Service (NMCS), executing the Navy's COMSEC programs. Additionally, the Navy Circuit Management Office (NCMO) and the Navy and Marine Corps Spectrum Management Center (NMSC) were also added to the NETWARCOM's increasing responsibilities. The disestablishment of COMNAVSECGRU in October 2005 added IO and Signals Intelligence (SIGINT) to NETWARCOM's growing mission. As the Capability TYCOM for C4I, NETWARCOM is responsible for:

1. Manning, equipping and training the Fleet in C4I.
2. Performing duties of Chief Operating Officer (COO) for the NNFE.
3. Developing and championing FORCEnet requirements.
4. Providing the FORCEnet operational architecture.
5. Serving as the operational agent for FORCEnet in Sea Trial.
6. Developing and implementing the Human Capital Strategy for Information Warriors.
7. Serving as the operational forces' advocate for development and fielding of information technology.
8. Operating, maintaining and defending Navy networks.

- 9. Conducting IO.
- 10. Conducting Space operations.
- 11. Performing duties as a Functional Component Commander to USSTRATCOM for Space, IO and Network Operations (NetOps).

**1.2.1 NAVAL COMPUTER AND TELECOMMUNICATIONS AREA MASTER STATION (NCTAMS)**

The NCTAMS operate and maintain responsive information transfer systems that provide real-time C4I information support to the Fleet.

There are two Master Stations:

- 1. NCTAMS LANT located in Norfolk, VA
- 2. NCTAMS PAC located in Wahiawa, HI

Each NCTAMS administers one of two Naval Communications Areas (NAVCOMMAREAs):

- 1. LANT: East of the Mississippi River to include LaMoure, ND to the Gulf of Oman
- 2. PAC: West of the Mississippi River to the East of the Gulf of Oman.

Fleet Commanders provide authoritative direction to the cognizant NCTAMS concerning coordinating and controlling classified and unclassified messaging, voice, data and video to ships, submarines, aircraft and ground forces operating worldwide in support of Naval and joint missions.

Each Naval Computer and Telecommunications Area Master Station (NCTAMS) provides operational guidance to area Naval Computer and Telecommunications Stations (NAVCOMTELSTA'S) as listed in Table 1-1. In the event of a catastrophe, the surviving NCTAMS or its alternate station, with direction from the cognizant Fleet Commander, will allocate remaining telecommunications resources among the surviving communications stations.

<b>NCTAMS LANT (NCTL)</b>	<b>NCTAMS PAC (NCTP)</b>
NCTS Jacksonville, FL	NCTS San Diego, CA
NCTS Bahrain	NCTS Guam
NCTS Naples, IT	NCTS Far East Yokuska, JA
NCTS Sicily	

**Table 1-1  
NCTAMS Operational Organization**

Each NCTAMS operates a Joint Fleet Telecommunications Operations Center (JFTOC) which functions as the primary control point for day-to-day operations within that NAVCOMMAREA. Each JFTOC is assigned a 24-7 Watch Officer. The responsibilities of the JFTOC Watch Officer are defined in paragraph 1.3.3.

Each NCTAMS and NTCS operates a Technical Control Facility (TCF) which contains the equipment necessary for ensuring fast, reliable, and secure exchange of information and typically includes distribution frames and associated panels, jacks, and switches and monitoring, test, conditioning, and order wire equipment. The TCF allows telecommunications systems control personnel to exercise operational control of communications paths and facilities, make quality analyses of communications and communications channels, monitor operations and maintenance functions, recognize and correct deteriorating conditions, restore disrupted communications, provide requested on-call circuits, and take or direct such actions as may be required and practical to provide effective telecommunications services.

Tech Control also performs basic functions for receiver and transmitter sites remotely. These include tuning, equipment patching, quality monitoring of received or radiated signals, switching or directional control of antennas, primary ship shore circuit operations, and the submission of required reports.

#### **1.2.1.1 NAVAL COMPUTER AND TELECOMMUNICATIONS STATION (NCTS)**

There are a total of seven NCTS' world-wide which are managed by and report to the two NCTAMS. They are strategically located around the world in customer concentration areas for ease in providing C4I support. Their primary mission is to provide the Navy Information Technology infrastructure and support services required for rapid and reliable voice and data communications within a specified Area of Responsibility (AOR).

#### **1.2.1.2 Navy Information Operations Command (NIOC)**

A total of fifteen NIOCs and sixteen subordinate detachments are located around the world to support Navy IO and SIGINT operations. These units provide IO planning, augmentation, Electronic Warfare (EW) support, Electronic Attack (EA), IO research, development, test and evaluation (RDT&E), and Computer Network Defense (CND) support. Of the fifteen, four NIOCs are located at National Security Agency sites to leverage National capabilities. These four sites, known as

regional NIOCs, are located in TX, HI, GA, and MD. Each of these four regional NIOCs incorporate a Fleet Information Operations Center (FIOC). FIOCs function as virtual Direct Support Elements (linguists, signals and nodal analysis) and provide target development and technical support to the fleet.

#### **1.2.2 NAVY CIRCUIT MANAGEMENT OFFICE (NCMO)**

It is the mission of the Naval Circuit Management Office to serve as the Department of the Navy (DoN) sole operational authority for all Naval Leased Terrestrial connectivity and serves as the DoN's primary agent to interact with DISA and commercial telephone vendors for coordinating DISN CORE data services and commercial leased connectivity.

Responsible for centrally funding and maintaining configuration management of all DoN's current and future leased terrestrial services. Delegated decision authority as OPNAV's agent to ensure the DISN CORE is efficiently and effectively implemented; collect, codify and provide information which supports current and future Department of Defense (DoD) efforts of cost alignment and circuit management; and to establish and maintain a complete DoN inventory of all DISN and commercial leased telecommunication circuits and equipments.

#### **1.2.3 NAVY MARINE CORPS SPECTRUM CENTER (NMSC)**

The Navy Marine Corps Spectrum Center (NMSC), formerly NAVEMSCEN, focuses on managing the DoN's use of the electromagnetic spectrum - a class of radio waves propagated by a system of electric and magnetic fields that includes the full range of radiant energy from radio and light waves to gamma and cosmic rays. Atmospheric interaction with these waves provides characteristics that can be harnessed, using electronic systems and devices, to transmit information.

Supporting the management and use of the radio spectrum means planning and coordinating joint use of required frequencies through operational, engineering and administrative procedures. The objective is to enable DoN spectrum-dependent systems and devices, such as radios that support voice communications or digital data links, Global Positioning System, and systems for detecting and suppressing enemy radar and communications sites, to perform their functions in the intended environments without causing, or suffering, unacceptable interference.

#### **1.2.4 NAVY COMMUNICATIONS SECURITY MATERIAL SYSTEM (NCMS)**

Navy Communications Security Material System (NCMS) administers the DoN Communications Security (COMSEC) program and is the Servicing Authority for DoN.



NCMS performs these specific functions:

1. Drafts and publishes COMSEC policy directives, standards, and procedures pertaining to COMSEC material security, distribution, training, handling, and accounting within the DoN.
2. Operates, maintains, and exercises administrative, operational, and technical control over the COMSEC Material.
3. Issuing Office (CMIO) for distribution of COMSEC equipment.
4. Develops procedures for and monitors compliance with proper physical storage and account management of COMSEC material.
5. Monitors compliance with national standards of the Protective Packaging Program for cryptographic keying material.
6. Reviews requests for and authorizes waivers to physical security requirements and the release of DoN COMSEC material to contractors.
7. Coordinates fleet requirements for the acquisition of all COMSEC material and publications for DoN Commands.
8. Establishes and disestablishes DoN Electronic Keying Material System (EKMS) numbered accounts.
9. Based on Combatant Commanders' requirements, ensures distribution of COMSEC material to Vault Distribution Logistics System (VDLS) components to ensure quantities are sufficient for EKMS account requirements, exercises, and contingency operations.
10. Provides status of Navy COMSEC material to EKMS accounts and planners.
11. Provides disposition instructions for DoN COMSEC material.
12. Evaluates instances of loss, compromise, and procedural violations of COMSEC procedures to determine the adequacy of existing procedures as well as overall compliance with existing policy.
13. Manages the CMS Advice and Assistance (A&A) Training Team program within the DoN, including training and certification of EKMS Inspectors.

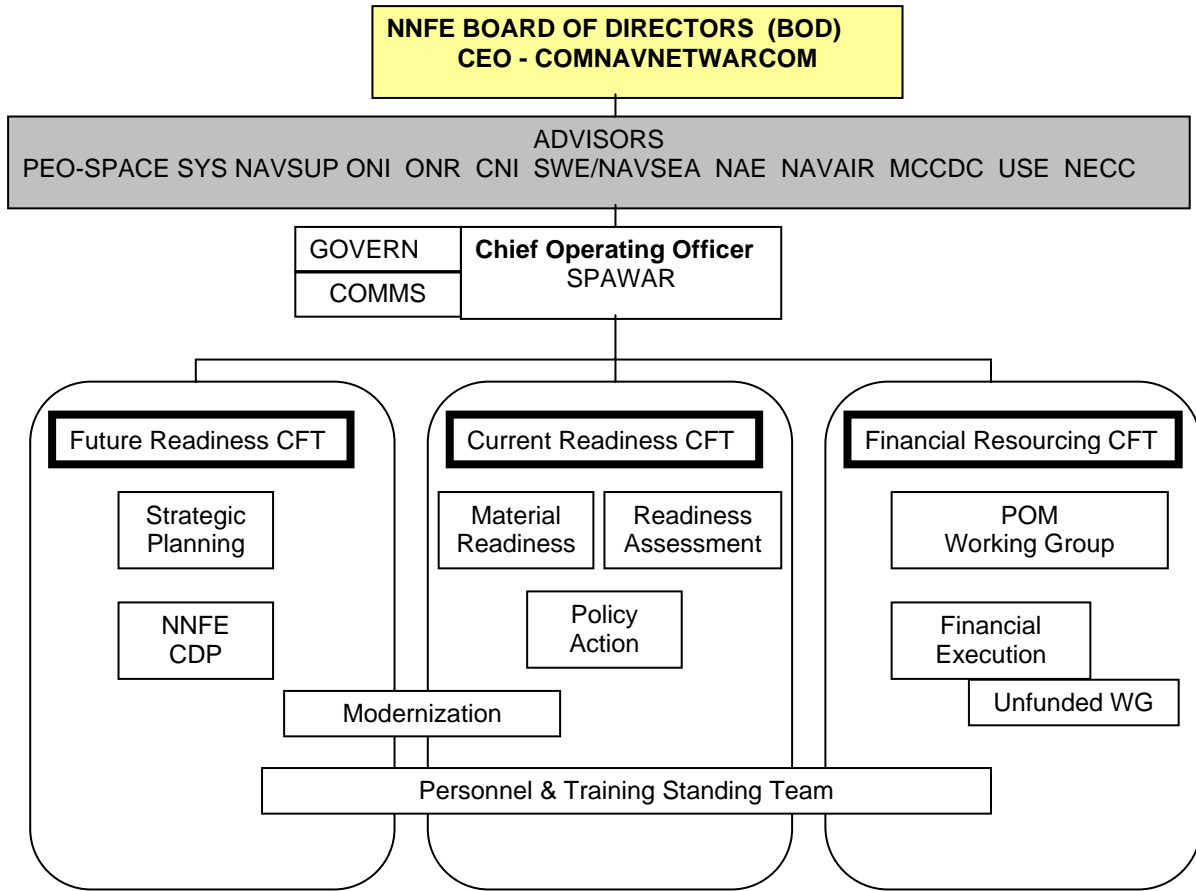
14. Conducts liaison and acts as the Technical Advisor with the Navy training community regarding the EKMS Manager Course of Instruction (COI) (V-4C-0013).
15. Is the Inventory Control Point (ICP) for COMSEC equipment throughout DoN and manages cryptographic equipment assets for DoN.
16. As the DoN Registration Authority, NCMS is responsible For registering using activities/commands with Tiers 1 And 0 and for assigning EKMS IDs to them. NCMS is also responsible for ordering initialization key for KPs and for maintaining registration data on its activities/commands.
17. FIREFLY POC (Point of Contact) for modern key privileges.

#### **1.2.5 NAVY CYBER DEFENSE OPERATION COMMAND (NCDOC)**

The NCDOC's mission is to coordinate, monitor, and oversee the defense of Navy computer networks and systems, including telecommunications and to be responsible for accomplishing Computer Network Defense (CND) missions as assigned by Commander, Naval Network Warfare Command and Commander, Joint Task Force - Global Network Operations (JTF-GNO).

#### **1.2.6 NAVAL NETWAR FORCENET ENTERPRISE (NNFE)**

The NNFE is an enterprise-wide approach to understanding the business of C5I and IO. It is a collaborative effort between NETWARCOM, SPAWAR, PEO C4I & Space, NAVSEA, OPNAV and other commands that provide C5I and IO support to the Fleet. The goal is to collectively develop processes, collaboration and metrics across the Enterprise to align the traditional functional commands and better understand the costs of conducting business and how it relates to readiness. This will, in turn, allow the Enterprise to make better decisions when applying critical resources, both dollars and manpower, while providing the right products and services to the warfighter faster and more efficiently. Figure 1-1 depicts the NNFE organization while Figure 1-2 provides a graphical representation of increased NNFE functions.



As Of 17 Oct 2007

**Figure 1-1  
NNFE Organization**

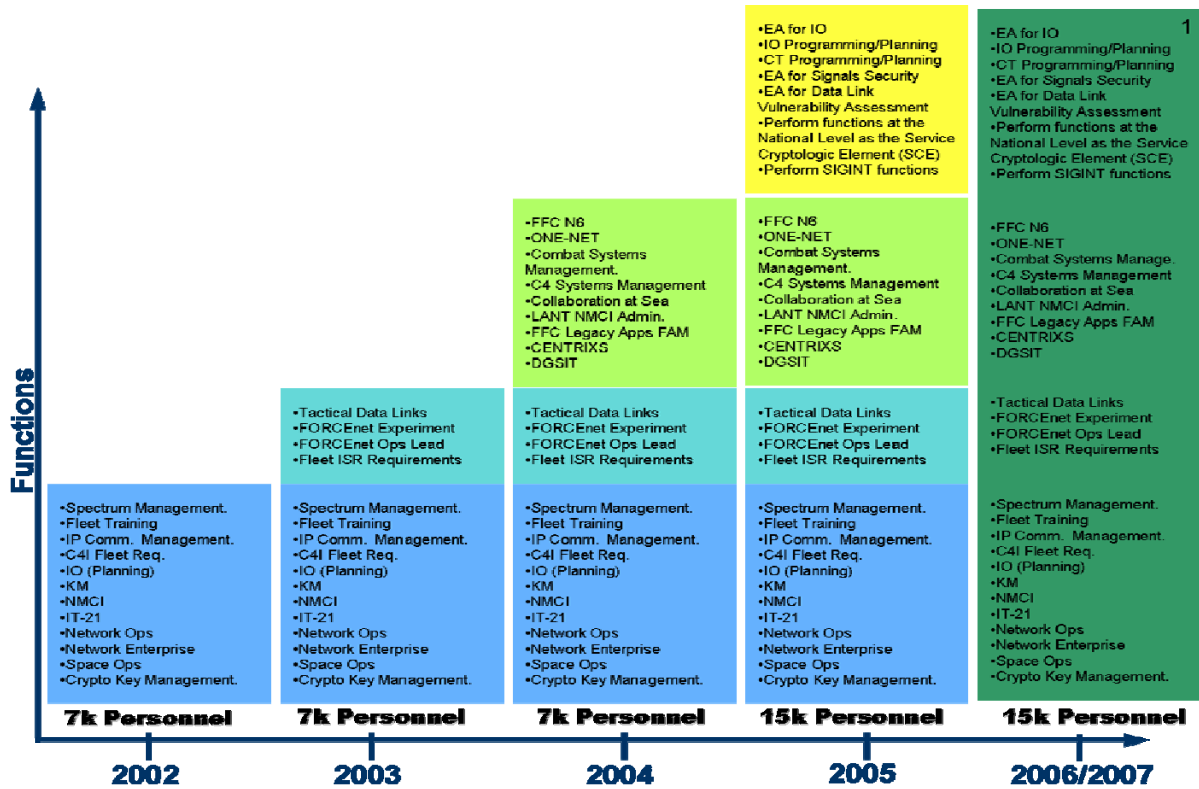


Figure 1-2  
NNFE Functions

### 1.3 BILLETS AND WATCHSTATIONS

The following sections describe both typical shipboard and shore communications billets. Shipboard and shore communications billets are similar in most respects. However, some billets may be shipboard only or shore only. Senior enlisted personnel may be assigned the duties normally assigned to officers when insufficient numbers of officers are unavailable to fill communications billets. Billet structures may differ from one ship/shore command to another depending on size and mission.

#### 1.3.1 COMMUNICATIONS OFFICER

The Communications Officer (COMMO) is responsible for the organization, supervision and coordination of the activity's communications in addition to management of connected internal radio systems. As an advisor to the Commanding Officer on all communications matters, the COMMO must be cognizant of all communications annexes of operational plans affecting the mission of the command and must maintain familiarity with communications sections of Naval Warfare Publications (NWP'S), Naval Telecommunications Procedures (NTP'S) and other associated communications publications. If

embarked, the COMMO is operationally assigned to the embarked staff to perform additional duties (ADDU). OPNAVINST 3120.20 (Standard Organization and Regulations of the U.S. Navy) contains additional COMMO duties.

### **1.3.2 RADIO OFFICER (RDO)**

The Radio Officer assists the Communications Officer by organizing, supervising and coordinating radio communications. The Radio Officer determines frequency plans, ensures all required circuits are manned; equipment is functioning properly, reviews tactical publications and fleet organization for pertinent information, conducts prescribed inspections and equipment inventories and conducts a technical training program for radio communications operating personnel. The Radio Officer is also responsible for the proper administration and processing of all Naval message traffic via automated delivery Local Area Networks (LAN).

### **1.3.3 JOINT FLEET TELECOMMUNICATIONS OPERATIONS CENTER (JFTOC) WATCH OFFICER**

The JFTOC Watch Officer is the Fleets 24/7 point of contact (POC) for any and all telecommunications anomalies and service requests at the NCTAMS. The JFTOC Watch Officer is the NCTAMS N3 primary assistant for supervising and coordinating all telecommunications functions ashore and maintaining a real-time, operational status of all circuits providing telecommunications services to the Fleet and other DoD and government customers. The JFTOC Watch Officer maintains Situational Awareness (SA) and directs actions to be taken to resolve COMMSPOTS, perform Communications Guard Shifts, activate and deactivate telecommunications circuits, and resolve telecommunications issues encountered by the Fleet. The NCTAMS JFTOC Watch Officers can be contacted at the following numbers:

NCTAMS LANT: 757-444-2124; DSN: 312-564-2124

NCTAMS PAC: 808-653-5377/1760; DSN: 315-453-5377/1760

### **1.3.4 ELECTRONIC KEYING MATERIAL SYSTEM (EKMS) MANAGER**

The Electronic Keying Material System (EKMS) is a centralized distribution and accounting system designed to provide appropriate safeguards for sensitive cryptographic publications, keying material, equipment and related devices. COMNAVNETWARCOM, as the Navy cryptographic authority, administers the EKMS system and approves doctrine. The Director, Naval Communications Security Material Systems (NCMS), a member of the COMNAVNETWARCOM organization, accomplishes the EKMS centralized accounting,

distribution and reporting functions. The Commanding Officer (CO) is responsible for command administration of allocated EKMS material. The CO must formally establish an EKMS account and appoint, in writing, an EKMS Manager and at least one alternate manager. The EKMS Manager is responsible for receiving EKMS material from the Communications Security Material Issuing Office (CMIO), maintaining accountability of all CMS material allocated to the command's EKMS account and reporting the status of the account to NCMS. The effective edition of EKMS-1 (series) contains specific EKMS Manager Qualifications and EKMS safeguard requirements.

### **1.3.5 INFORMATION ASSURANCE MANAGER (IAM)**

The primary mission of the Information Assurance Manager (IAM) is Information Security (INFOSEC). The IAM is responsible for the overall security of the NIPRNET and the SIPRNET Local Area Networks (LAN). Security personnel working for the IAM monitor the activity of all users on the LAN to include any potential external/internal network attacks (hackers). The IAM is also responsible for ensuring the anti-virus programs on all LANs are updated regularly. Additional responsibilities are to conduct training during command indoctrination, conduct INFOSEC training with the Information Assurance Officers (IAO), establish and implement the Configuration Control Board (CCB), manage the Life Cycle Management (LCM) for all systems, procure additional hardware/software/resources, approve or disapprove any Abbreviated Systems Decision Papers (ASDP), maintain the Command software and hardware inventory, and maintain the accreditation for all LANs/computer systems on board the command.

### **1.3.6 COMMUNICATIONS WATCH OFFICER (CWO)**

Under the Communications or Radio Officer, the CWO is operationally responsible for all incoming and outgoing traffic and the day-to-day operation of the Communications Center. The CWO serves as the representative of the communication/radio officer during periods of watch, assuming general charge of all communication activities of the command. The CWO expedites outgoing and incoming traffic, ensures delivery of messages to appropriate personnel, supervises cryptographic processing of messages, serves as the primary source of information on message inquires, enforces communications security, investigates and corrects communications delays, failures and violations and advises message originators on proper preparation of messages.

The CWO, under the guidance of the Communications Officer, is responsible to the Staff Duty Officer (SDO)/Command Duty Officer (CDO)/Officer of the Deck (OOD) for:

1. Ensuring that communications capabilities are ready to match the mission and tasks of the command.
2. Maintaining, understanding and ensuring compliance with all applicable rules, regulations, procedures and current communications directives, e.g., effective operation orders, communications plans, call signs, recognition procedures, authentication and similar material.
3. Monitoring the performance of the watch by inspecting spaces, spot-checking logs closely observing personnel and procedures at irregular intervals, sampling performance factors such as internal message handling times, equipment/system activation or alignment times and making periodic inquiries to users of remote controlled communications circuits.
4. Coordinating with the appropriate Joint Fleet Telecommunications Operations Center (JFTOC) Watch Officer as required and reporting unusual communications difficulties or discussing rerouting/reallocating existing resources for optimum afloat support.
5. Monitoring the Fleet Broadcast and coordinating with the JFTOC Watch Officer on broadcast shifts.
6. Being aware of the status of message backlogs, high precedence messages, and messages requiring special handling.
7. Being aware of circuit outages or difficulties and their causes.
8. Being aware of the status of communications reports and taking appropriate action to ensure timely reporting for:
  - (a) General quarters (shipboard).
  - (b) Material conditions of readiness.
  - (c) Darken ship (shipboard).
  - (d) Underway, anchoring, or mooring (shipboard).
  - (e) Eight o'clock reports.
  - (f) Emergencies (drill or actual).
  - (g) Emergency destruction (drill or actual).

**1.3.7 SYSTEMS TECHNICAL CONTROL SUPERVISOR**

The Communication Systems Technical Control Supervisor is responsible to the CWO. The Systems Technical Control Supervisor is responsible for but not limited to the following duties:

1. Directs control, operation and patching of long-haul communications media (including satellite) and local circuits;
2. Manages selection of transmitting, receiving and terminal equipment, use of cryptographic equipment including shifts and adjustments and all equipment on the air;
3. Ensures reliable communications through familiarity with all possible combinations of antennas, transmitters, receivers, frequencies, and terminal equipment;
4. Directs circuit and system performances tests, ensures that corrective action is taken in case of circuit outages and that control links and land lines are properly used;
5. Coordinates operational changes on circuits with subscribers;
6. Inspects and maintains logs and records of data pertinent to control center operations;
7. Maintains watch to watch integrity of administration, operational and cryptographic publications and materials;

**1.3.8 COMMUNICATIONS CENTER SUPERVISOR**

The Communications Center Supervisor is responsible to the CWO for:

1. Managing the overall operation of the telecommunications facility;
2. Supervising message processing and circuit operations;
3. Directing action to prevent or reduce backlogs;
4. Monitoring the performance of the watch;
5. Notifying the CWO of all matters of an unusual or urgent nature;



6. Maintaining required logs and files;
7. Coordinating circuit problems with the technical control supervisor;
8. Other duties as the CWO may assign.

#### **1.3.9 AUTOMATED DATA PROCESSING OFFICER (ADPO)**

The ADP officer is responsible for ensuring the ships networks operate in an efficient manner. Ensuring effective use of disk space and ensuring back ups are conducted on a routine basis. The ADPO serves as the focal point and source of expert technical information pertaining to information systems planning, development, operation and standardization. Additionally:

1. Directs the installation, maintenance, and repair of automated data processing equipment and tactical data systems equipment to include their peripherals;
2. Determines maintenance action required;
3. Oversees required maintenance history reports and maintenance program routines;
4. Supervises the acquisition of ADP equipment;
5. Liaisons with systems manufacturer representatives;
6. Responsible for LAN configuration;
7. Coordinates with embarked staffs (CSG/ESG/MEU, etc) to ensure adherence to command policy and guidance to maintain configuration control;
8. Drafts Memorandum of Agreements between the ship and embarked staffs.

#### **1.3.10 SYSTEMS ADMINISTRATOR**

Systems administrators maintain, and operate numerous [computer](#) systems, [networks](#) and their associated peripherals. Systems administrators are tasked with installing, supporting, and maintaining [servers](#), Local Area Networks (LAN) and other computer systems, and planning for and responding to service outages and other problems. Systems Administrators are responsible for planning for and responding to service outages and other computer and/or network problems. Other duties may include [scripting](#) or light [programming](#), [project management](#) for systems-related projects, supervising or training computer operators, and

being the consultant for computer problems beyond the knowledge of technical support staff.

#### **1.3.11 KNOWLEDGE MANAGEMENT (KM) PROCESS AND ORGANIZATION**

Knowledge Management refers to a range of practices used by organizations to identify, create, represent, and distribute knowledge for reuse and learning across the organization.

Knowledge Management programs are typically tied to organizational objectives and are intended to lead to the achievement of improved performance, tactical or competitive advantage, and higher levels of innovation.

While knowledge transfer (an aspect of Knowledge Management) has always existed in one form or another, for example through on-the-job discussions with peers, formally through professional training and mentoring programs, and technologically through knowledge bases, and other knowledge repositories, knowledge management programs attempt to explicitly evaluate and manage the process of creation or identification, accumulation, and application of knowledge or intellectual capital across an organization.

The Knowledge Manager will ensure that all of the pillars of knowledge management are addressed. However, the Strike Group Knowledge Manager should not conduct or lead every "hotwash" event or evaluate every existing and new strike group process for improvement. Instead, he/she ensures that an internal strike group process exists for others to perform these functions.

It has been consistently demonstrated that a prerequisite for Knowledge Management success is the sincere support and enthusiastic involvement of senior leadership. Organizationally, this is demonstrated by having the Knowledge Manager (KM) report directly to the Chief of Staff and/or Commander. Practically, this means the KM consistently engages senior leadership in each Knowledge Management effort. As part of the Commander's personal staff, the KM and his/her team is more likely to retain an enterprise perspective, critical when developing and implementing solutions that will affect the entire strike group organization.

It is important to share the responsibility of Knowledge Management throughout the strike group organization and beyond. Although it is the KM with the title several other personnel and organizations are built to support knowledge management initiatives and knowledge flow. For example, knowledge flow may occur by education, training, research, discussion, and trial and error. Strike group education and

training starts in the schoolhouse and continues through the Fleet Readiness Training Plan (F RTP) cycle (refer to paragraph 1.6.9.3). A Training Officer is attached to each unit and staff, research is handled by Systems Commands (i.e., SPAWAR), discussions, trial and error will occur without a KM assigned. However, the KM should monitor these contributions and work closely with contributors to ensure the strike group obtains maximum benefit from each.

### **1.3.12 INFORMATION MANAGEMENT (IM) PROCESS AND ORGANIZATION**

Information Management (IM) is the handling of information acquired by one or many disparate sources in a way that optimizes access by all who have a share in that information or a right to that information. At a training command currency, accuracy and availability of information is critical to effective training and support of the fleet. IM Organization should consist of the following:

- Information Management Officer (IMO)
- Command Security Manager
- Information Assurance Manager (IAM)
- Syndicate Heads
- N7 Representative

The document management strategy will provide an overarching guide for management of electronic documents and images. This strategy will include the following elements:

1. Storage - Where will documents be stored?
2. Retrieval - How can people find needed documents?
3. Filing - How do we organize our documents?
4. Security - How do we protect against loss, tampering, or destruction of our documents? How do we keep sensitive information hidden and protected?
5. Archival - How do we ensure availability of historical documents in the future? How do we protect our documents against inadvertent destruction or deletion?
6. Retention - How do we decide what documents to retain? How long should they be kept? How do we remove them afterwards?
7. Distribution - How do we get documents into the hands of the people who need them?

8. Workflow - If documents need to pass from one person to another, what are the rules for how their work should flow?
9. Creation - If more than one person is involved in creating a document, how will they collaborate?

Effective collaboration requires six essential elements:

1. Roadmap for Evolution - A clear plan must be developed for the effective development and implementation of new processes and an understanding of the organizations affected by these changes.
2. Collaborating Communities - Each role in the collaboration process must be identified, defined and understood.
3. Process Structure - There must be a clear understanding of exactly what points in our training process require collaboration.
4. Clearly Defined Interfaces - Specifics around the collaboration itself. What is the purpose of each point of contact? Who is interacting with whom? What are the roles and responsibilities of each person or organization involved?
5. Vehicles for Collaboration - Standard means of capturing and sending information must be identified and used. What system (email, calendar, CaS, KWeb, SIPRNET, NIPRNET, etc) will be used?
6. Enabling Technology - The technical infrastructure (applications, services, security, networks, etc.) must be in place to ensure that the process and the collaboration within the process can be executed effectively.

### **1.3.13 STAFF COMMUNICATIONS OFFICER**

The Staff COMMO advises and assists staff, fleet, or force commanders by planning and administering communications. Duties included formulating communications plans and directives, maintaining liaison with other Services, Joint or Allied commands on communications matters. The staff COMMO must report upon the expected effect communications conditions as they relate to the performance of the command in a present or anticipated mission. He/she reports to the commander through the organizational channels of the staff. The Staff COMMO prepares all communications orders, plans, instructions and other documents necessary to carry out assigned missions or tasks. These are usually prepared as

communications annexes to operational plans or orders, but a command may establish standard communications plans or procedures to significantly reduce the number, size or complexity of the communications annexes to operational orders.

When a staff embarks on a ship, the ship's communications organization is usually transferred for temporary additional duty (ADDU) to the embarked commander. The Staff COMMO then works closely with the ship's COMMO in prescribing watches, message handling procedures and other details to maintain effective communications. The Staff COMMO is also responsible for providing the Commanding Officer of the flagship with appropriate communications services. The Staff COMMO must exercise care to maintain the communications organization and files of the flag ship intact so that if the embarked staff moves, the ship's communications organization can effectively resume operations.

The Staff COMMO may issue instructions to subordinate units as authorized by the unit commander only, and in the latter's name, e.g., communications procedures, setting or securing of watches, frequency shifts or circuit discipline. However, he/she cannot issue instructions directly to personnel in other ships/units. Any such orders must be in the name of the commander and through the chain of command to the Commanding Officer of the ship/unit in question.

#### **1.4 ADMINISTRATION**

##### **1.4.1 COMMUNICATIONS EQUIPMENT POPULATION SUMMARY (CEPS)**

Communications Equipment Population Summary (CEPS) is a complete list of communications equipment on board ship. This summary reflects the ships communications capabilities and limitations. CEPS are submitted two times each year, after significant C4I upgrades and two months prior to an extended deployment. Instructions for submitting CEPS are outlined in GCIB 22 Kilo.

##### **1.4.2 MATERIAL SUPPORT**

Material support of the communications complex is the effort directed toward maintaining facilities in peak operating and physical condition. The three most important keys to successful material support are system operation, preventive maintenance, and casualty control. The success of these efforts depends largely upon how well the operating and maintenance personnel coordinate and carry out these responsibilities.

The system approach to material support considers

operational procedures and personnel turnover and provides for continued training of new personnel to replace those who leave. Without thorough operator training, the total system cannot function effectively. An operator must demonstrate the ability to align a system in accordance with specified operating instructions before being considered qualified in that system. Formal instruction and on-the-job training must emphasize the following:

1. Detailed alignment procedures.
2. Quality control monitoring procedures.
3. Technical limitations of the system.
4. General care and cleanliness of the system components.

Planned Maintenance System (PMS) pertains to the planning, scheduling, and managing resources (personnel, material and time) to perform those actions which contribute to uninterrupted functioning of equipment within its design characteristics. The PMS system provides each command, department, and supervisor with the means to plan, schedule, and control maintenance with appropriate schedules. PMS pertains to preventive maintenance rather than corrective maintenance based upon the requirements contained in Ships Systems Command Manuals, manufacturers' instruction books, other associated publications, and Reliability Center Maintenance (RCM) analyses.

1. The Department Head uses the Maintenance Material Management (3-M) Manual OPNAVINST 4790.4 (series), normally kept in the departmental office, to plan and schedule maintenance. The 3-M Manual contains a short description and frequency of equipment maintenance requirements, a list of Navy-wide 3-M contacts, and a summary of 3-M forms.
2. The Cycle Schedule displays preventive maintenance requirements based on an overhaul cycle. Each work center prepares a cycle schedule, which is used to make out the quarterly schedules.
3. The Quarterly Schedule displays the current quarter's maintenance schedule. The Cycle and Quarterly Schedules are contained in a display holder known as the "Maintenance Control Board", which is usually located outside the department office. Maintenance requirements on this board reflect the overall preventive maintenance program for the department.
4. The Weekly Schedule is posted in each space with a copy of the applicable portions of the PMS Manual. This schedule contains all planned maintenance to be

accomplished within the week for equipment in that space. It assigns individual personnel to perform specific maintenance on specific equipment on a particular date. The Leading Petty Officer or 3-M Supervisor for the department assigns the work and records its completion on the schedule.

5. The Maintenance Requirement Card (MRC) defines the planned maintenance assignments in sufficient detail to enable personnel to perform the tasks without difficulty. It lists the enlisted rate, time, tools, parts, and materials required to perform the maintenance. A complete deck of all MRC'S is kept in the department office. If a card is lost, soiled, or torn, it can easily be replaced by duplicating a copy from the master deck. Some of the benefits realized from PMS include increased reliability, increased economy, convenient programming of work by advance planning, and better records.
6. The Maintenance Data System (MDS) provides the Navy with a system for recording the expenditure of resources (personnel, material, and time) associated with certain categories of maintenance actions. In addition, it provides retrievable data concerning common malfunctions, enabling designers to document and issue field changes on present equipment, and to assist in selecting and designing future equipment.

Casualty control is the process which assures that system failures are reported, the casualty is restored, and the system is operationally tested prior to being placed in service. The casualty must be reported to the Commanding Officer, the OOD and/or other appropriate personnel and must include the exact extent of the casualty, the estimated time of repair, and the circuits/capabilities affected by the casualty. Reporting procedures are contained in NWP 1-03.1. When afloat units experience communications casualties that impact directly on the communications system's traffic delivery requirements, i.e., broadcast and ship/shore capabilities, the unit must inform the area NCTAMS of the casualty via COMSPOT message (see Appendix B of this publication).

#### **1.4.3 CORRECTIVE MAINTENANCE**

Corrective maintenance is often required to restore a piece of equipment to an operational status after a breakdown, or when the inspection cycle indicates a corrective action must be performed to ensure reliability. Only trained, technically competent personnel who have demonstrated the ability to perform such functions should perform this corrective maintenance.

All corrective maintenance actions will be maintained in divisional logs and used as a reference in subsequent casualty reports (CASREP).

#### **1.4.4 INVENTORY CONTROL**

Procedures for inventory control are specified in NAVSUP P-485, Afloat Supply Procedures, and NAVSUP P-1, Naval Supply Systems Command Manual.

Prompt repair of inoperative or malfunctioning equipment is dependent upon adequate spare parts support. To provide each command with support for the installed equipment, an allowance of repair parts is stocked as recommended by the Coordinated Shipboard Allowance List (COSAL) or in the case of shore activities the Coordinated Shore Based Allowance List (COSBAL). These allowance lists are adjusted to a prescribed range and depth of stocked parts based on the usage rate obtained by correct failure reporting as prescribed in the 3-M system. As new stock level requirements are determined, the command allowance list is updated.

An adequate supply of consumable items used in daily operation such as paper, pencils, log and record forms, printer ribbons/cartridges, and cleaning supplies must be maintained to prevent interruption of telecommunications facility operations.

#### **1.4.5 COMMUNICATIONS PUBLICATIONS**

NAVWARDEVCCEN has converted all communications publications from paper/microfiche/CD ROM to electronic copies available on the World Wide Web (WWW). Cognizant authorities will accomplish routine changes to communications publications by issuing a complete new publication(s) via the World Wide Web. Urgent changes will be promulgated via message corrections. These corrections should be kept with the publication until they are incorporated into the next issue.

Message corrections to publications are identified by a numerical sequence consisting of a two number designation separated by a slant sign. The first number indicates the sequential number of the message correction to the original or revised publication. The second number is the change which will incorporate the material, e.g., MC 7/3 is the seventh message correction and will be incorporated into the publication by change number three.

The person designated to update a publication must take extreme care to enter/file the message or printed change correctly. For printed publications, NTP 1-01 provides general guidance but the following rules are also



applicable:

1. Affixing a correction as a cutout is preferred to using a flap. If there is no room for a cutout, the flap will be attached to the binder side of the page.
2. All material superseded by a correction will be lined out prior to inserting a cutout or flap. One diagonal line through the superseded information with the correcting individual initials is sufficient.
3. Lengthy pen-and-ink corrections should be typed and pasted in publications as a cutout/flap.
4. Rather than use glue or gummed tape, rubber cement or mucilage is preferred for entering corrections. This allows easy removal of the cutout/flap if required by a subsequent change. Also, gummed tape often causes pages to stick together or results in torn pages when the cutout or flap is removed.
5. After entry of a pen-and-ink, cutout or flap correction, the source of the correction will be noted in the margin adjacent to the entry (e.g., MC 7/2). Complete information on the authority for the change will be listed on the record of changes and corrections page in the front of the publication.
6. A page check is required on all publications after entering a page change and will be recorded on the record of changes and corrections page in the front of the publication. Residue from the page change will be page checked prior to destruction.

When authorized by the foreword or letter of promulgation of a publication, extracts may be made to disseminate information. Extracts will be assigned a classification based upon the highest classification assigned the articles or paragraphs from which the information is taken. The responsibility for controlling extracts from publications rests with the command. The extract will be clearly marked with its appropriate classification, and safeguarded locally in the manner prescribed for its parent document.

When recommending changes to these publications, the letter of promulgation provides relevant information. Proposed changes to Navy Telecommunications Publications (NTP) may be submitted via email to NNWC(underscore)POLICY@navy.mil or by posting a comment in the blog on NNWC SNEWS website.

To provide positive control of communications publications, a publication inventory sheet will be used. For 24 hour per day telecommunications facilities where publications are continually available for use, a watch-to-watch inventory

will be used. At the change of each watch, the watch supervisors will jointly conduct a sight inventory of every publication. Some loose-leaf distributed publications require a page check at each watch change in addition to the sight inventory. These loose-leaf publications will be specifically indicated on the watch-to-watch inventory sheet. Signing of the watch-to-watch inventory sheet by the relieving watch certifies that the publications were sighted, the required page checks were conducted and that the relieving watchstander is responsible for them. Any discrepancies noted will be resolved prior to relieving the watch. All signatures will be in ink. Watch-to-watch inventories of communication publications may be destroyed after 30 days provided they are no longer required by local procedures. For situations where a 24 hour communications watch is not kept, a daily inventory is required on those days the publications are actually available for use, e.g., at a telecommunications facility open Monday through Friday 0800-2000.

Submit proposed changes to communications publications through the normal chain of command to the cognizant authority of the publication in question (found in the letter of promulgation). The preface of NTTP 1-01 contains information for submitting change recommendations to tactical publications. Additionally, the current NTTP 1-01 contains information on the reviewing, updating, distributing, and handling tactical warfare publications.

## **1.5 SAFETY**

### **1.5.1 SAFETY PRECAUTIONS**

Safety is a major responsibility of all personnel. Because of the dangers involved in working with electronic equipment, certain safety precautions must be observed to prevent exposure to radiation, radioactive components, or lethal voltages. Each person concerned with electronic equipment must make it their responsibility to understand and practice prescribed precautions. U.S. Navy Regulations, chapters 3 and 7 of OPNAVINST 3120.32, OPNAVINST 5100.19, are explicit in delineating the responsibility of personnel to concern themselves with accident prevention.

### **1.5.2 GOING ALOFT**

When personnel must go aloft, permission in writing must be obtained from the OOD, CWO, Combat Information Center Watch Officer (CICWO), Engineering Officer Of The Watch (EOOW) and other divisions as necessary to ensure all safety precautions have been met (during underway periods, the Commanding Officer is the only person who can authorize

permission to go aloft). The aloft sheet will be initialed by all concerned to indicate knowledge of aloft/down status. While in port, permission should also be obtained from adjacent ships.

While aloft, all personnel are required to wear a safety harness.

Personnel are not permitted to go aloft when any antenna in the immediate vicinity is energized by a radio or radar transmitter, unless it is determined in advance that no danger exists. This includes the antennas of a ship moored alongside or across the pier, or in some cases nearby shore radio stations.

Warning signs and suitable guards must be provided to prevent personnel from coming into contact with high voltages. Equipment must be tagged conspicuously and not energized while repair personnel are aloft. In addition to the electrical hazards involved, precautions must be taken to prevent the rotation/ radiation of radar sets that could physically knock personnel from their working platform or expose them to hazardous emissions. All radar cutout switches should be turned on prior to getting on radar platforms. Ship-wide announcements should be broadcast via the 1-MC every 15 minutes by the OOD while personnel are working aloft.

### **1.5.3 DANGEROUS VOLTAGES AND CURRENTS**

Voltage levels encountered in electronic equipment are extremely dangerous. NEVER WORK ALONE. A small amount of current passing through a vital part of the body can cause death. Fatal shock depends on the resistance of the human body; however, fatalities from exposure to as low as 30 volts have been recorded.

Removing a unit or part from its normal location and energizing it while it is outside its normal cabinet or cover bypasses all designed safety and protection features, such as interlocks, grounds, and enclosures. If personnel must remove and energize a unit or part, take special safety measures - ground the chassis and frame of all power supplies and high-voltage units removed for servicing and ground all circuits normally grounded in operation whenever power is applied to the unit. Hazardous voltages may occur in faulty equipment at points where only low voltages are normally encountered.

Provide warning signs and guards to keep personnel from accidentally contacting dangerous voltages and inadvertently contacting energized antennas.

When working on equipment where the power has been secured,

personnel must tag the switch to prevent accidental energizing of the equipment while repairs are in progress. OPNAVINST 3120.32 (Standard Organization and Regulations of the U.S. Navy) contains detailed TAG-OUT requirements and procedures.

#### **1.5.4 DISCHARGE AND GROUNDING CIRCUITS**

The charge retained by electrical machinery and equipment after it is secured is sufficient to cause a shock that could result in death or serious injury. To be safe, discharge and ground all machinery, power tools, capacitors, and high voltage leads in radio equipment before cleaning or attempting repairs. Use an insulated lead or shorting bar for this purpose. Repeat the discharge operation several times.

#### **1.5.5 ADJUSTING ELECTRONIC TRANSMITTING EQUIPMENT**

No person should reach in or enter energized equipment enclosures for servicing or adjusting, except as prescribed by official technical manuals and when specifically authorized by the Commanding Officer. When work on energized electrical or electronic equipment is necessary and authorized, observe these common precautions:

1. Station a person by the circuit breaker or switch ready to cut the power in case of an emergency;
2. Have a person qualified in first aid standing by during the entire period of repairs;
3. Provide ample illumination;
4. Remove all metal objects from clothing and body;
5. Insulate worker(s) from ground with dry wood, rubber matting, a sheet of phenolic insulating material, or several layers of sandpaper or dry canvas;
6. Cover metal tools with insulating rubber (non-friction) tape;
7. Work with one hand only;
8. Wear rubber gloves if nature of work permits; if not, wear a glove on the hand not holding tools;
9. Be extremely careful not to touch the metal shielding shells of capacitors, klystrons, cathode-ray tubes, and other components which are at high potential above ground.

### **1.5.6 RADIO FREQUENCY RADIATION HAZARD**

All personnel must be constantly alert to transmitting equipment causing hazardous voltages to build up in a ship's standing rigging and other portions of the ship's superstructure. These voltages will cause shock or produce open sparks when personnel or conductive material makes contact. Do not operate transmitters while combustibles or electrically activated ordinance are within the minimum safe distance prescribed.

See appropriate specific NAVSEA Technical Manuals (NSTM'S) for detailed instructions.

### **1.5.7 DISPOSAL OF RADIOACTIVE ELECTRONIC PARTS**

Transfer radioactive electronic parts, e.g., electron tubes to an activity licensed by the Nuclear Regulatory Commission or to a Nuclear Regulatory Commission land-disposal site. Accomplish disposal of these items by sealing them in a sturdy, leak-proof container marked to indicate radioactive content and transferring them to a naval shipyard or supply activity for ultimate disposal per existing directives. If breakage should occur, clean all contaminated areas thoroughly and handle waste materials as described above. Personnel must wear safety glasses and gloves when handling this material.

## **1.6 TRAINING AND READINESS**

### **1.6.1 GENERAL**

The key to successful communications operations is the training and qualification of communications personnel at all levels. Any command, afloat or ashore, achieves maximum communication effectiveness, regardless of the communications set-up, when all personnel are thoroughly trained and qualified in the operation and maintenance of installed systems.

### **1.6.2 TRAINING DOCUMENTS**

Prior to developing any successful training package, identify the skills and knowledge level required to adequately perform each task. NAVPERS 18068, Navy Enlisted Manpower and Personnel Classifications and Occupational Standards, provides the Navy's statement of minimum requirements for enlisted skills.

After identifying skill requirements, refer to any of the following references for formal training or training by other means:

1. NAVEDTRA 10500, Catalog of Navy training courses (CANTRAC), provides a consolidated list of formal training locations and courses available. It also has information on Navy enlisted codes (NEC) awarded to trainees.
2. If formal training is not available, refer to NAVEDTRA 10061, the list of training manuals and correspondence courses, for an alphabetical list of personnel qualification standards (PQS) and computer-based training (CBT) programs.
3. OPNAVINST 3500.34, Personnel Qualification Standards program explains the requirement to locally develop PQS and produce PQS-type manuals entitled "Job Qualification Requirements (JQR)".
4. Additional sources of training material available for use at individual commands include type commander instructions; check off lists, training booklets and technical manuals which provide detailed instructions that can be adapted to local training programs. Communications Information Bulletins (CIB), and Communications Information Advisories (CIA) issued by the area NCTAMS as well as Navy Telecommunications Directives (NTD) issued by COMNAVNETWARCOM are also good sources of information for training.

### 1.6.3 PERSONNEL TRAINING

Training is a major factor contributing to battle readiness. The prime objective of training is to increase the ability of personnel to operate and administer the facilities of the command effectively under all conditions. Long range training programs for communications personnel must contain provisions for general training, including examination for advancement in rating, qualification for assigned watches, damage control, first aid, and fire fighting. An essential portion of the training program should be the effective cross-training of communications personnel within functional areas, so that all Information Systems Technician will be qualified to assume any of the duties in radio spaces. Each command must pursue a vigorous training program consistent with the required training as outlined in OPNAVINST 3120.32. The Communications Officer, under the Commanding Officer, is responsible for proper performance and training of personnel in the communications department.

Informal quizzes that are normally oral should be given frequently to ensure personnel are familiar with equipment characteristics, total system operation, casualty control, circuit procedures, etc. All communications personnel must

have access to and read publications dealing with frequently used procedures or equipment.

Drills are an important means of ensuring proficiency especially in areas of contingency communications, equipment or personnel casualty and emergency destruction. Drills must emphasize response to emergencies or orders for destruction by billet, rather than by name. The designation of primary and alternate billets to carry out specific tasks allows for the absence of a particular individual.

There is a natural tendency to keep people in jobs with which they are familiar. This stems from a desire to achieve and maintain a smoothly working unit, division or team. Such action, however, limits the scope of knowledge of the individual, does not make provision for casualty replacement, and generally impedes advancement. To offset this tendency, make a plan to rotate personnel to ensure complete coverage of all jobs. Personnel should attain thorough qualification before rotating from one job to the next. Personnel who are best qualified to do the job should provide initial instructions to trainees. Record the completion of personnel qualification cards in individual service records because they provide ready reference to the status of an individual's qualifications.

The Command Readiness Training Team (CRTT), a component of the Type Commander (TYCOM) Readiness Management System (TRMS) is an essential element of training assessment and evaluation within the command. The CRTT is an asset that can be used to determine current training proficiencies and levels of readiness through drills, critiques, and documentation validation on a department, division or watch section basis.

#### **1.6.4 NCMS ASSIST VISIT (CMS A&A Team)**

A NCMS assist visit by a qualified EKMS inspector is required every 18 months for commands holding EKMS material. Approximately 8 months prior to the next required visit, a command should receive a copy of the NCMS visit outline. This serves as a reminder to schedule the visit and since the outline is used by the NCMS visit team, the custodian should review it prior to the team's arrival. The results of a NCMS visit are reported only to the Commanding Officer to allow the command to recognize and correct any problem areas.

Because the purpose of a NCMS visit is to assist the command in the proper maintenance of its account and associated cryptographic material and equipment, these visits offer a unique training opportunity to custodians and alternates.

They are particularly helpful prior to extended deployments or within six months of assuming responsibility for an account.

NCMS assist visits are not inspections. Inspections are normally unannounced. There are 10 CMS A&A Teams (NCMS Washington DC, NCTAMS LANT Norfolk VA, NAVCOMTELSTA San Diego CA, NAVCOMTELSTA Jacksonville FL, Pearl Harbor HI, COMSUBGRU 2 Groton CT, Camp Lejuene NC, NAVCOMTELSTA Puget Sound WA, NAVCOMTELSTA Naples IT and NAVCOMTELSTA Far East JA. Each CMS A&A Team is responsible for providing COMSEC/EKMS training, Advice and Assistance (A&A) to all numbered DoN EKMS accounts and local elements.

#### **1.6.5 COMMUNICATIONS ASSISTANCE TEAM (CAT)**

CAT visits present an invaluable opportunity for shipboard personnel to confer with shore based naval communicators on operational matters. CAT's provide advice on current communications procedures, e.g., SHF, FSM or broadcast management, and can also analyze and identify shortages in ship's equipment. Ships can use the results of such visits to document requirements for spare parts, repair equipment or to modify existing COSAL'S.

#### **1.6.6 EMBARKABLE-STAFF INTEGRATION TEAM (ESIT)**

ESIT assists the embarking staffs (CSG, ESG, CVW, etc) and ships/units in developing a migration plan to support the pending embarkation. This includes addressing ISNS, NTCSS and NMCI related issues.

Specifically the ESIT mission is:

1. Instructs ship and embarking staff personnel on proper integration of Information Systems onto ISNS networks to ensure expeditious shore to ship transition.
2. Provide onsite shipboard support during the actual embarkation and provide follow-on support as required.
3. Provide onsite support during the re-integration of deployed assets as required.
4. Analyze integration issues and provide guidance for resolution in accordance with SPAWAR Configuration management.
5. Develop, document and maintain procedures for configuring the embarking forces equipment, software and for configuring ship's equipment to support the embarkation process.



## ESIT responsibilities:

1. Provide a structured Internet Protocol (IP) address scheme based on addresses issued to ship.
2. Assist with switch configuration to support embarking staffs.
3. Assist with New Technology (NT) configuration of workstations and servers to include network services like Domain Name System (DNS), Windows Internet Name Service (WINS), and email.
4. Establish NT domain trusts between ship and embarking staff domains.
5. Provide an after action report on each assist visit for ship and embarking staff personnel to use as a reference for subsequent embarkations.
6. Assist with coordinating mail exchange (MX) record and DNS record shifts at area NOCs.
7. Assist with submitting Naval Change Requests (NCR) and Engineering Change Proposals (ECP) to provide solutions for network infrastructure deficiencies and discrepancies.
8. Assist with the release of Fleet Advisory Messages (FAM) as they pertain to embarkations.

Units request ESIT support via naval message.

TO: COMSPAWARSYSCOM SAN DIEGO CA//PMW160//  
 SPAWARSYSCEN CHARLESTON SC//847/847NC//  
 INFO SHIP  
 EMBARKABLE STAFF/UNIT  
 RESPECTIVE FLTCDR  
 RESPECTIVE TYCOM  
 COMNAVNETWARCOM NORFOLK VA  
 BT  
 UNCLAS  
 MSGID/  
 SUBJ/EMBARKABLE STAFF INTEGRATION TEAM SUPPORT REQUEST//  
 RMKS/**DESCRIBE NATURE OF VISIT, TO INCLUDE DATES AND  
 EMBARKABLE STAFF TO BE INTEGRATED.**  
 BT

**\*\*Request should be submitted at earliest convenience, but NLT 7 days prior to requested assist. This will ensure all preliminary work required is completed and minimize scheduling conflicts.**

ESIT will respond to the support request via naval message,

hours and dates of operation are outlined in the message. ESIT performs pre-site survey of the units shore commands and deployed destinations (buildings and ships) to ensure proper hardware and software configuration and functionality. Refer to the ESIT Support CONOPS for more detailed outline of what ESIT can do.

#### **1.6.7 TEAM OSCAR**

Team Oscar provides the fleet with information technology support through proactive interaction with ships and embarked staffs by a team of area NCTAMS technical experts. Team Oscar provides solutions and in-depth coordination on EHF, SHF, UHF DAMA, NIPRNET/SIPRNET, ADNS, T-1 connectivity and message processing.

#### **1.6.8 EQUIPMENT TECHNICAL ASSIST VISITS**

Regional Maintenance Centers (RMC) are responsible for providing technical assistance and repair of USN surface and subsurface units. They support Continental United States (CONUS) maintenance and repair activities and report the status of all active maintenance actions. The RMC's are also responsible for the coordination of diving, salvage and towing support operations. They are the first point of contact when units require technical assistance. Should an RMC representative determine that they are unable to effect repairs for whatever reason, then the RMC will send a message passing the tasking and funding to the applicable In-Service Engineering Agent (ISEA).

Fleet System Engineering Team (FSET) personnel are contracted by the government to provide technical support to the fleet. Every deployed strike group has at least two (2) FSETs assigned to the strike group staffs on aircraft carriers and large deck amphibious ships. These technical experts can tap into all SPAWAR resources to aid in troubleshooting all complex network and command, control, communications, computer, and intelligence (C4I) issues.

#### **1.6.9 EXERCISES AND TESTING**

Exercises and testing are designed to examine a strike group's readiness to deploy.

**1.6.9.1 COMMAND ASSESSMENT OF READINESS AND TRAINING (CART)**

To gain maximum benefit from limited training time and resources, a ship must enter each training cycle with a clear understanding of what specific training is required and a detailed plan for accomplishing it. CART is a two-part event intended to help the ship meet this objective.

1. During CART I, normally conducted during the first half of Fleet Readiness Training Plan (FRTTP), the ship looks ahead with its strike group commander and air wing and lays out a proposed schedule for major events.
2. CART II will be conducted aboard a ship no earlier than 90 days prior to Tailored Ship's Training Availability (TSTA) I. The purpose of CART II is to ensure the ship is ready to conduct training and prepare a detailed, tailored schedule for the unit level phase of the training cycle. It is imperative that TYCOM, ATG, Strike Group Command and Air Wing Commander's representatives be integrally involved with the ship during CART II.

**1.6.9.2 NAVY MISSION ESSENTIAL TASKS (NMET)**

The Navy Mission Essential Tasks List (NMETL) measures the effectiveness of a strike group's readiness to deploy. The NMETL provides guidelines for training in order to prepare for deployment. The drills are normally conducted during COMPTUEX/ESGEX and graded by COMSTRKFORTRALANT/PAC (CSFTL/CSFTP).

The NMETL defines essential tasks, conditions, and standards that support the capabilities Fleet Forces will need to deter and defeat adversaries. The mission capability specified in the NMETL defines the requirements that the inter-deployment training cycle should prepare forces to execute.

The NMETL will serve as the Fleets' common baseline of tasks, conditions, and standards for use in planning, conducting, assessing and evaluating fleet training. Mission essential tasks are defined as those mission analysis approved by CFFC that are absolutely necessary, indispensable, or critical to the success of a mission. The NMETL will be the vehicle that ensures common fleet training and resultant operational practices in both Atlantic and Pacific fleets.

### **1.6.9.3 FLEET READINESS TRAINING PLAN (FRTP)**

The numbered fleets and leading TYCOMs developed the six-plus two CSG capabilities through the creation of the FRTP, a 27-month cycle that replaces the old Inter-Deployment Training Cycle (IDTC). The FRTP consists of four phases: Maintenance, Unit Level Training, Integrated Training, and Sustainment. The maintenance phase is followed by a period of unit-level training to achieve a level of readiness for the Carrier Strike Group to be considered "Emergency Surge Capable." The idea is to have the major prerequisites for a surge deployment (manning, maintenance, and training) completed so that additional tailored training can be completed quickly if necessary to surge the CSG due to a crisis or contingency operation. The Integrated phase of training is tailored to individual ship and air wing strengths and weaknesses and concludes after completion of COMPTUEX (C2X) and air wing training at Naval Air Station Fallon. At this point a CSG is considered Surge Ready, meaning it could deploy on short notice if required. The sustainment part of the FRTP consists of a variety of training evolutions designed to maintain a CSG's readiness until it actually deploys, and might include a Joint Tactical Fleet Exercise (JTFEX). The FRTP is an adjustable and scalable approach to training that ensures Naval capabilities are aligned with mission essential tasks and potential operational tasking. By the nature of their location, Forward Deployed Naval Force (FDFNF) units have different training opportunities available to them as compared to CONUS units. However, their Operating Tempo (OPTEMPO) affords them the opportunity to maintain tactical proficiency through dedicated training event and in conjunction with regional and exercise commitments. This results in a balanced training program between available schoolhouse and on-the-job training.

### **1.6.9.4 JOINT TASK FORCE EXERCISE/EXPEDITIONARY STRIKE GROUP EXERCISE (JTFEX / ESGEX)**

Joint Task Force Exercise (JTFEX), is a requirement for deployment readiness. JTFEX is an advanced scenario-based Task Force exercise emphasizing command and control relationships within the Joint/Coalition task force. JTFEX is also comprised of mission-sets described in CSFTL/CSFTPINST 3501.1 enclosure (1) and contained entirely within the context of a 4-6 day battle problem scenario.

It is important to the United States Joint Forces and our Coalition partners that we as a Navy become proficient in the operation of equipment and systems that are not used in every day information exchange.

Expeditionary Strike Group Exercise (ESGEX) is a requirement for amphibious deployment readiness. Marine Corps landings and communications exercises are performed during ESGEX. These scheduled at-sea tests and evaluations are designed to assist USN/USMC operators and technicians in identifying C4I/Combat system interoperability issues.

#### **1.6.9.5 COMPOSITE TRAINING UNIT EXERCISE (COMPTUEX)**

COMPTUEX is orchestrated by Commander Strike Forces Training LANT/PAC (COMSTRKFORTRALANT/PAC) (CSFTL/CSFTP)). The exercise is the integrated phase underway portion of the Fleet Response Training Plan (F RTP), which fully integrates the CVN-CVW and coordinates single/multi-ship training within the carrier strike group (CSG) CWC organization.

CSFTL/CSFTP, as Deputies for Training for Commander Second Fleet (C2F) and Commander Third Fleet (C3F) respectively have responsibility for the integrated strike group training phase of the F RTP. CSFTL and CSFTP have developed and maintain the Navy Mission Essential Task (NMET) based training standards for Strike Group staffs, Warfare Commanders, and supporting Warfare Coordinators and are resident at the Navy Tactical Information Management System (NTIMS) website, or CSTFL/P CAS websites. The NMETs are broken down and assigned to mission-sets/events and form the foundation of training requirements contained in the integrated training event playbook found in CSFTL/CSFTPINST 3501.1 (series).

#### **1.6.9.6 DEPLOYING GROUP SYSTEMS INTEGRATION TESTING (DGSIT)**

The DGSIT process follows the concept that the Strike Group's interfacing sensors and networks are considered as one total Combat/C4ISR system, designed to function in a seamless and complementary manner. DGSIT is designed to assist operational commanders and systems Program Offices in ensuring installed C4I and Combat Systems are ready to support operational force war fighting requirements. This concept was developed in response to the Fleet's request for a technical demonstration of "Total Strike Group" Combat/C4I system functionality following new system installations and upgrades prior to the final phases of the Inter-Deployment Training Cycle (IDTC).

The DGSIT process assists the Commanders, TYCOMs, and SYSCOMs (including Program Executive Office's) in the coordination and programming of existing support processes, assists operators in assessment of validation during underway operations.

The process is chartered and funded by Commander Naval Network Warfare Command.

#### **1.6.9.7 FINAL INTEGRATION TESTING (FIT)**

FIT is the at-sea event phase of the DGSIT process designed to identify C4I/Combat systems interoperability and integration issues at a CSG/ESG Force level. It is conducted post-target configuration date (TCD) typically during COMPUTEX/ESGEX. During FIT, the DGSIT Team (comprised mostly of system knowledgeable Subject Matter Experts (SME)) conducts coordinated test events and individual system evaluations during underway operations.

#### **1.6.9.8 UNIT LEVEL TRAINING READINESS ASSESSMENT-CERTIFICATION AND UNIT LEVEL TRAINING READINESS ASSESSMENT-SUSTAINMENT (ULTRA-C / ULTRA-S)**

Unit Level Training Readiness Assessment Certifications. ULTRA-C is conducted by the ISIC, supported by ATG and CLASSRON.

Approximately every two years, ships will undergo an ULTRA-C, followed by an ULTRA-S every six months. The purpose of the ULTRA is to validate the ship's ability to self-assess and train, and to certify the ship's ability to perform required missions to a set standard. Continuous training will permit the Surface Force to maintain unit level training readiness at higher levels throughout the training cycle.

#### **1.6.9.9 FXP 3 CCC DRILLS**

The Fleet Exercise Publication (FXP) is designed to provide exercises that will support the training of units in each of their naval warfare mission areas and required operational capability/projected operational environment. FXP 3 contains instructions for conducting command, control, and communications (CCC) series exercises. These exercises should be conducted on a frequent basis to train newly reporting personnel as well as a workup toward the graded exercises for the departmental Combat Systems Green "E" Award.

#### **1.6.9.10 C4I FAST CRUISE**

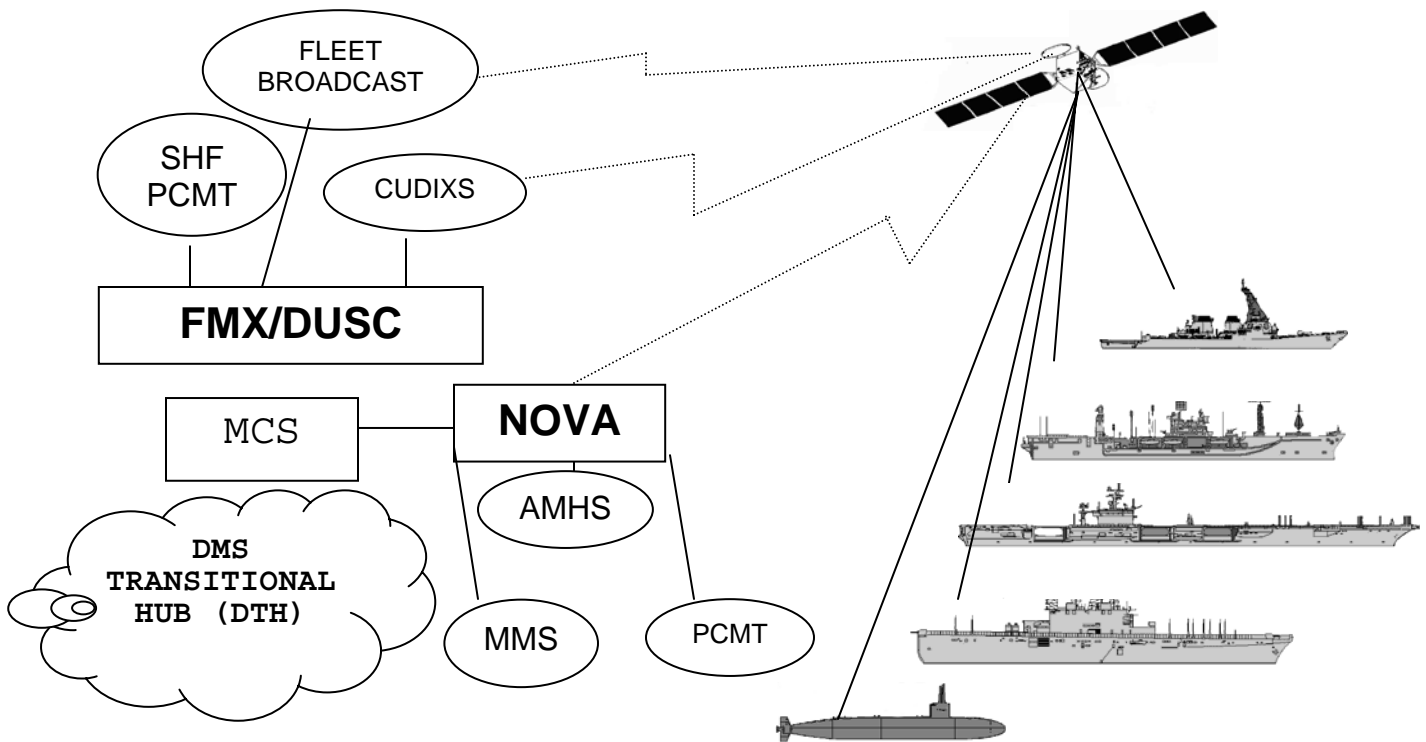
C4I fast cruise is designed to light off and test equipment with all members of the strike group (when feasible) while moored to the pier and at least 96 hours prior to an underway period. The purpose of the fast cruise is to train personnel in the setup and operation of circuits and equipment that will be utilized during the upcoming underway/deployment.

**CHAPTER 2**  
**AUTOMATED COMMUNICATIONS**  
**AND**  
**INFORMATION SYSTEMS**

**2.1 AUTOMATED COMMUNICATIONS SYSTEMS - GENERAL**

Using the Defense Information Infrastructure (DII) as a backbone, the Navy has designed automated systems ashore and afloat to process message traffic with minimal intervention by communications personnel. Figure 2-1 depicts the system flow. This chapter describes these systems, providing information to the communicator to assist in effective management of these systems.

The Navy's automated software based communications systems are dynamic. To keep these systems current users can propose improvements or report defects in the software systems used by the Navy.



**Figure 2-1**  
**Message Traffic Process**

## 2.2 MESSAGING SYSTEMS

One of the most important concepts of operating in an organization that is spread across the globe is not just the ability to communicate, but to communicate quickly, effectively, securely, and with full accountability. With the development, fielding, and proliferation of Internet Protocol (IP) based communications (i.e. E-mail and Internet Relay Chat), the desire is to quickly share information by any means available and people do.

With that in mind, the average user would think that with all of the e-mail and chat going on in the Navy that record message traffic would soon be replaced. To the contrary, Navy personnel have not only continued to use record message traffic, but have exceeded the capabilities of messaging systems and their associated communications paths.

With constantly stressed low data rate (LDR) communications networks such as the Common User Digital Information exchange Subsystem (CUDIXS), the need to maximize use of the "new" IP paths has become a driving force in the future of Naval Messaging. Even with existing systems (i.e. pre-DMS) we find the need to adapt to our available resources.

### 2.2.1 DMS OVERVIEW

The DMS employs the messaging and directory services using internationally recognized COTS-based X.400 and X.500 messaging and directory products. The DMS COTS baseline, which includes DoD military messaging, directory, and security enhancements, provides the messaging infrastructure for DoD electronic organizational messaging support. The DMS messaging and directory components are managed and protected by specialized systems management and security support mechanisms and components. The DMS management system uses system management tools and message tracing applications to isolate and identify problems and to report on the health and welfare of the DMS infrastructure.

Protocols and components of the Multi-level Information Security Service Initiative (MISSI) provide DMS security services. The MISSI Message Security Protocol (MSP) and the Fortezza encryption card provide encryption and digital signature services. Each Fortezza card contains encryption keys that are based on the organization or command's authorized level of clearance and digital certificates that are unique to the card's assigned organization. A designated Certification Authority (CA) uses a CA Workstation (CAW) to generate and post the encryption keys and digital certificates to the organization's Fortezza card and to the DMS X.500 directory. The MSP and the Fortezza card generate and exchange security tokens that support the exchange of digitally signed and encrypted messages between DMS users.



DMS network transport services are provided by the Defense Information Systems Network (DISN) and secure dial-up connections. DoN users receive DMS services or enabling capabilities through the allocation of various levels of messaging, directory and network management services, and DISN network or dial-up connectivity.

#### **2.2.1.1 TACTICAL MESSAGE GATEWAY (TMG)**

The MFI is an infrastructure-level component that provides protocol conversion between the DMS MTS and the DTH legacy-messaging environment. The MFI is the primary means of providing interoperability with DTH users that have not migrated to DMS, including the Allied and tactical users. MFI'S are typically located in DISA managed DMS Transition Hubs (DTH), which include legacy switching centers, or Navy LNOSC locations. The DMS automatically routes messages through an MFI whenever the recipient's DMS X.500 directory address contains a legacy preferred delivery attribute.

#### **2.2.1.2 CERTIFICATION AUTHORITY WORKSTATION (CAW)**

The CAW is a National Security Agency (NSA) certified and approved workstation that provides enabling technology that supports messaging security services of confidentiality, integrity, authentication, and non-repudiation. Organizations use the CAW for programming identities onto Fortezza Cards, generating public-key certificates, and posting security information to the DMS X.500 directory. An appointed CA is responsible for operating the CAW, programming Fortezza cards, and using the CAW along with an ADUA to post certificates and security information to the DMS directory.

#### **2.2.1.3 MESSAGE CONVERSION SYSTEM (MCS)**

Currently, the Defense Message System-Message Conversion System (DMS-MCS) is operational at the DISA DTH located at Fort Detrick MD. As fielded, the DMS-MCS is comprised of the Message Conversion System Message Processor (MCSMP), the MCS Directory Component (MDC), the Central Directory Component (CDC), and the Update Authority Component (UAC). The UAC portion of the DMS-MCS is located at NCTAMS LANT and NCTAMSPAC. The Navy has fielded Regional MCS' at the two NCTAMS. The Regional MCS configuration consists of the MCSMP and the MDC. Changes were made to provide supportable, removable hard drive capability and to provide a Mode I interface to the NOVA System. Although the UAC and CDC are not considered part of the Regional MCS configuration, the Regional MCS receives Plain Language Address (PLA) updates from the CDC via the SIPRNET.

The primary purpose of the Regional MCS is to provide PLA-to-Routing Indicator (RI) look up and assignment. After receiving a message from the host NOVA System, the Regional MCS will validate the message, assign the appropriate RI(s) and return the message

to the NOVA for delivery. If invalid PLAs are found by MCS, the MCS will automatically generate a service message to the originator. Each invalid PLA will receive a RI of RUBDPLA side routed on the original message. The MCS provides a means of inserting Routing Indicator(s) (RI'S) in an ACP128 formatted message based on the PLAs contained in that message. Currently, any U.S. General Service (GENSER) subscriber employing ACP128 format and sending narrative pattern traffic may, upon approval, use the DMS-MCS for PLA-to-RI conversion. Both the Navy Regional MCS and DMS-MCS are transitional systems to aid customers in the migration from AUTODIN to DMS. Even though these systems are transitional, both are designed to remain viable until the phase-out of the AUTODIN system is completed.

#### **2.2.1.4 DMS AND TACTICAL DMS PROXY AFLOAT SYSTEM**

The Tactical Messaging DMS proxy system at TMG sites provides the ability to interface and translate DMS messages to and from tactical units, using approved DMS infrastructure components. The NCTAMS sites have a direct interface to legacy systems and have the Tactical Messaging DMS proxy capability which is supported by the Integrated Shipboard Network System (ISNS) hardware with software provided by the Common PC Operating System Environment (COMPOSE).

#### **2.2.1.5 DEFENSE MESSAGE DISSEMINATION SYSTEM (DMDS)**

DMDS is an end user message profiling application that automatically profiles and disseminates a command or organization's incoming message traffic. The organization can configure DMDS to distribute the profiled messages in either encrypted or unencrypted form. If DMDS distributes encrypted messages, all recipients will need Fortezza security services. Organizations must protect local networks that distribute unencrypted DMS messages in accordance with guidelines set forth in OPNAVINST 5239.1.

#### **2.2.1.6 MAIL LIST AGENT (MLA)**

The MLA provides a collective addressing capability for DMS. The MLA receives messages addressed to a collective address called a Mail List and redistributes them to those recipients who are members of the Mail List. The Mail List in DMS is similar to the Address Indicator Groups (AIG), Collective Address Designators (CAD), and task force designators (TF) used in the DTH legacy system. The MLA accepts delivery of a message addressed to a Mail List only from the user(s) authorized to submit messages to that Mail List. The MLA adds each member of the Mail List as a recipient to the message. If it is an encrypted message, the MLA generates a token for each recipient so recipients can decrypt the message.

#### **2.2.1.7 DIRECTORY SYSTEMS AGENT (DSA)**

The DSA serves as a repository for the DMS directory information. This information, known as the Directory Information Base (DIB), contains organizational user attribute information such as the organization's directory name, digital certificates, network address information, and administrative information such as telephone numbers and mailing addresses. The DIB is distributed throughout the directory system in multiple DSA'S. Users access the DSA through the IDUA, a directory browser application.

#### **2.2.1.8 BACKBONE MESSAGE TRANSFER AGENT (BMTA)**

BMTA'S function as high-level message store-and-forward switches within the DMS MTS. BMTA'S are installed at DMS infrastructure level sites (i.e., Defense Information Systems Agency (DISA) Regional Network Operations and Security Centers (RNOSC) and Regional Nodes (RN)). BMTA'S serve as independent store-and-forward message switches between LNOSC'S, USMC LCC'S, major claimant sites, and DISA operated DMS infrastructure sites. BMTA'S are generally downward connected to one or more LMTA'S or primary GWS'S and either laterally or upwardly connected to other BMTA'S. The BMTA receives messages from other BMTA'S located throughout the global DMS infrastructure and routes them according to specific routing algorithms.

#### **2.2.1.9 LOCAL MESSAGE TRANSFER AGENT (LMTA)**

The LMTA functions as an intermediate-level message switch that stores and forwards messages across a fully interconnected switch fabric called the MTS. LMTA'S typically reside at LNOSC sites and store and forward message traffic destined to and from DMS specialty products (i.e., PUA, Mail List Agent (MLA), MultiFunction Interpreter (MFI)). LMTA'S are bound to a local DMS Directory System Agent (DSA) and make routing decisions based on specific information stored in the X.500 directory.

#### **2.2.1.10 HIGH ASSURANCE GUARD (HAG)**

The DMS HAG is a secure "gateway" component installed in the DMS secret messaging domain that selectively allows or denies message exchange between DMS NIPRNET and SIPRNET messaging domains. The HAG examines each message to ensure that:

1. The organization has digitally signed and encrypted messages exchanged between NIPRNET and SIPRNET domains.
2. Message originators and recipients are authorized to exchange messages between the DMS NIPRNET and SIPRNET messaging domains.
3. All exchanged messages via the HAG are appropriately marked as unclassified.

4. Messages exchanged between the two messaging domains may include file attachment(s) if the rules listed below are followed:
  - a. Attachment types must be limited to specific file extension types authorized by the organization as being crucial to mission accomplishment.
  - b. All messages must be signed and encrypted with hard-token Class IV Fortezza to provide authentication and non-repudiation.
  - c. The DMS HAG must be capable of decrypting messages to ensure attachments are of the appropriate types and to perform a dirty word search.
  - d. The organization must define the HAG Access Control List (ACL) to limit the users who can send attachments from low to high.

The HAG also passes directory information between specific directory servers in the two messaging domains. Unclassified directory information for message recipients in both messaging domains is accessible to users on the NIPRNET. Changes and updates to the unclassified directory information are passed through the HAG to the SIPRNET domain through a process known as directory shadowing.

#### **2.2.1.11 SERVICE MANAGEMENT SYSTEM (SMS)**

The SMS supports monitoring and control of DMS components at various management levels. The SMS is comprised of a data base system as well as specialized message trace applications, directory administration tools, and fault management applications for collecting data and reporting on the status of DMS components. The SMS message trace and fault management applications run on a DMS component called the Management Workstation (MWS). Directory administration is performed using a DMS component called the Administrative Directory User Agent (ADUA). The MWS also incorporates a trouble ticket system for tracking and managing system problems and outages. The SMS applications and its MWS and ADUA hardware component systems are typically installed at Navy LNOSC locations and USMC Control Centers.

#### **2.2.1.12 GROUPWARE SERVER (GWS)**

The GWS is a component that stores and forwards messages from the DMS client to Primary Groupware Servers (PGWS) or Local Message Transfer Agents (LMTA). The GWS, PGWS, and LMTA all serve as store-and-forward message switching devices within the DMS architecture. The GWS operates at the lowest level in the DMS Message Transfer System (MTS). The GWS provides direct message store-and-forward support to DMS clients. The PGWS and LMTA

provide second echelon message store-and-forward support to local or remote GWS'S. The GWS, PGWS, and LMTA components are frequently co-located at sites with large concentrations of DMS clients. Typically, these components will be centrally located at Navy LNOSC'S. The USMC typically will deploy GWS'S down to the major command level. DMS clients must use dial-up connections whenever DISN network connectivity is not available and the GWS is remotely located.

### **Message Store (MS)**

The MS serves as an intermediary between the DMS client and a GWS. The MS resides on the GWS and serves as an electronic mailbox for the DMS client. The MS or GWS mailbox accepts and stores messages on behalf of the organization until recipients download and delete the messages.

### **DMS Client or User Agent**

The client, sometimes referred to as the User Agent (UA), is a software application installed on a DMS-compliant hardware platform. The DMS client enables the preparation, review, release, submission, delivery, storage, archiving, display, and printing of DMS messages. A single hardware platform and a single DMS client application may support multiple users. The DMS client also contains an Integrated Directory User Agent (IDUA). The IDUA function allows the user to search the directory for addressing information that can be added directly to drafted messages or cached in the user's Personal Address Book (PAB) for later use.

### **2.2.2 TROUBLE MANAGEMENT SYSTEM (TMS)**

To support the goal of increased reliability, Enterprise Network Management System (ENMS) has been fielded with a Trouble Management System (TMS) as an integral part of the network management tool set. TMS is based on the commercial "Remedy" product that is used extensively in the private sector to provide relevant data on network performance. TMS will be used by the shore establishment to track, from inception to completion, all events impacting service to individual or multiple units. ENMS will build databases that identify trends and provide hard data on performance that our current infrastructure is incapable of doing. That will aid in decision making about where to expend our precious fiscal and manpower resources to improve C4 service to the warfighter.

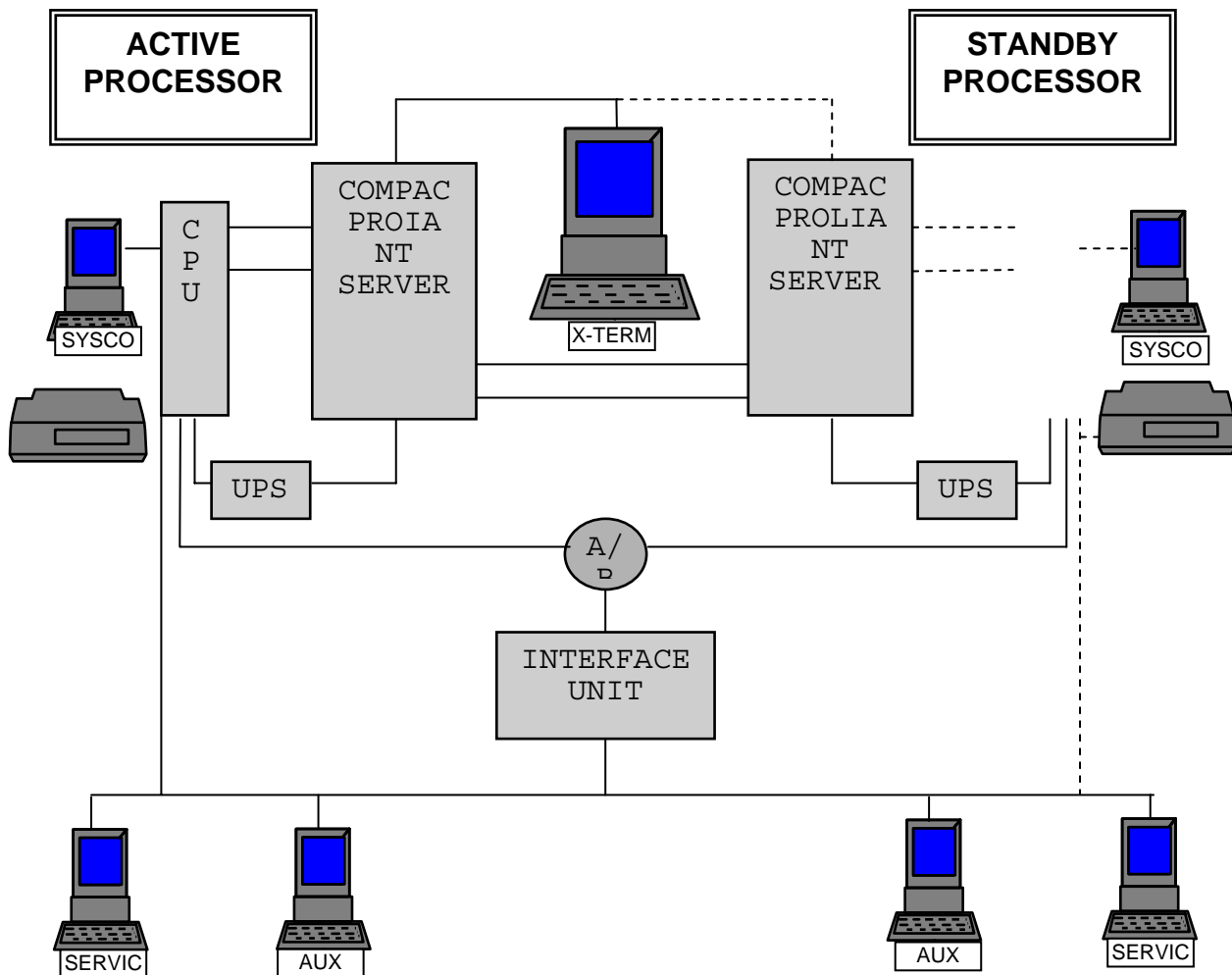
As with any automated system, the manner in which data is entered is critical to its success. TMS has the capability to automatically extract data from COMSPOT reports and fleet service advisories when presented in specific formats. To realize the capabilities that TMA offers, message drafters must take great care to ensure that data fields relevant to the incident at hand are formatted as directed herein. Messages not properly formatted

will result in delayed action due to unnecessary human intervention.

For COMSPOT reporting format and further guidance refer to Appendix B.

### **2.2.3 AUTOMATED MESSAGE STORE AND FORWARD (NOVA)**

NOVA is a UNIX based, base-level Mode 1 store and forward terminal (Figure 2-2) dependent on the worldwide switching functions of the DTH to relay messages to other commands outside the immediate area of responsibility, services and agencies. NOVA is a store and forward switching system that provides automated readdressal and quote functions for authorized users. For message accountability purposes, the system assigns a unique Processing Sequence Number (PSN) to each message received. This PSN provides a means of message recall and is used as part of an automated readdressal or quote request. NOVA provides duplicate checking and First-In First-Out (FIFO) by precedence processing. Received messages are sorted by routing indicator and delivered to the DTH and backside terminals, using Mode 1 protocol. NOVA performs validation of format lines 2 through 4, 12a, 12b, 15 and 16 of ACP 128 messages. Messages found to be in error are diverted to a Service Intercept Position (SIP) for manual intervention. If the message cannot be corrected at the SIP the message will be serviced by the NOVA operator. Installation of the NOVA Virtual Circuit Protocol (VCP) brings a Local/Wide Area Network interface into the NOVA application in addition to the AUTODIN Mode One interface. Use of this interface reduces the number of connections to the DTH.



**Figure 2-2**  
**Nova Configuration**

#### 2.2.4 PERSONAL COMPUTER MESSAGE TERMINAL (PCMT)

PCMT is a microcomputer-based message processing system designed for low-volume telecommunications facilities. This store-and-forward processing system is operated by message center or fleet center personnel. PCMT provides exchange of messages between the telecommunications facility and user organizations using diskette media, Secure Telephone Units (STU) III or dedicated connectivity.

#### 2.2.5 GATEGUARD

GateGuard serves as the primary legacy system interface point for DoN Organizations. It provides a gateway communication link from the AUTODIN Subscriber Terminal (AST) (e.g., Nova, MDT or PCMT) to an organization's Automated Information System (AIS) or Office Automation System (OAS). GateGuard was the first DoN messaging system to fulfill the "idea" of extending messaging services to the user level. Traffic received by the Nova, MDT or PCMT can be transferred electronically to GateGuard, which will ensure only

traffic of a classification level not exceeding that of the OAS communications line is transferred. GateGuard is capable of processing Unclassified to Top Secret SPECAT A type messages.

GateGuard can function as either a dedicated delivery device (paper or diskette) or as a gateway. The GateGuard system is composed of three elements: A Guard Device (for use on dedicated links), an AUTODIN Gateway Terminal (AGT), and a Gateway Communication Link to an arbitrary AIS. The AST communication link uses Local Digital Message Exchange-Remote Information Exchange Terminal (LDMX-RIXT) communication protocol. To the AST, GateGuard appears to be an attached RIXT and is also capable of providing a Mode I interface to suitably equipped hosts. The AGT is designed for operation by an organization's administrative personnel. The AGT can provide paper or diskette media for message dissemination within the organization. GateGuard exchanges data with the supporting AST using the communications link or diskette media. Unless a DMS-approved automated message release capability is available on the AIS, messages cross the communication link from the GateGuard to the AIS in one direction. The GateGuard performs the following functions:

1. Audit Trail.
2. User Identification.
3. Message Storage and Retrieval.
4. Format Checking.
5. Security Checking.
6. Precedence Notification.
7. Message Routing.
8. AST Mode I Interface.

If the communications link between GateGuard and the AST is not contained entirely within controlled spaces, it must be covered by approved communication security (COMSEC) equipment. The circuit must be covered even if only UNCLASSIFIED messages are exchanged. A KG-84 may be used to cover a circuit that will carry messages of any classification. STU III may be used to cover circuits that pass messages classified up to and including TOP SECRET.

#### **2.2.6 FLEET MESSAGE EXCHANGE (FMX)**

Fleet Message Exchange (FMX) replaced the Naval Computer Processing and Automatic Routing System (NAVCOMPARS). Whereas NAVCOMPARS consisted of five, loosely joined sites using similar



applications, FMX implemented a tightly integrated system of two sites running identical, interacting applications and using a worldwide tactical network to share data and resources. The FMX application rides on a layer of trusted, advanced commercial off-the-shelf (COTS) software: two UNIX operating systems, a Relational Database Management System (RDBMS), TCP/IP based LAN software, and an X Windows Graphical User Interface (GUI). The application operates on a platform of advanced computers connected locally by an Ethernet LAN and worldwide by the Defense Information Systems Network (DISN). Figure 2-3 depicts the in-line system configuration.

Two operating sites have been established for FMX; one at NCTAMS PAC Honolulu, HI and NCTAMS LANT Norfolk, VA. FMX consists of three separate components. One of these is a new system that is responsible for keying the fleet broadcast (BCST) and providing the necessary functionality to support the fleet broadcast requirements. This component is the Fleet Broadcast Keying System (FBKS). To reduce development time and need for operator interaction, FBKS was developed as a simple store and forward system. It runs on the same hardware platform as DUSC. Although FBKS and DUSC are functionally separate systems, they share the same database and use the same message parsing and validation software.

FBKS is connected on the backside of the NOVA system. In addition to providing the interface to FBKS, NOVA system provides the interface to the existing Common User Digital Information Exchange System (CUDIXS) and provides routing and alternate routing between circuits for FBKS and CUDIXS.

#### **2.2.7 DIRECTORY UPDATE SERVICE CENTER (DUSC)**

The Directory Update and Service Center (DUSC) is a multi-purpose system that will produce directory updates for the Defense Message System (DMS) Update Authority Component (UAC) and database updates for the FMX. The updates will be automatically produced from communications guard shift messages and collective update messages. DUSC will also process communications guard list request messages and allow operators to service fleet messages with errors found by the DMS Message Conversion System (MCS). DUSC performs the following functions:

1. Provides for operation of the service message center.
2. Produces directory updates for the DMS UAC from Communications Guard Shift (COMMSHIFT) messages and Collective update messages.
3. Produces database update messages for FMS and FMX systems.
4. Processes Communications Guard List (COMMGRDLST) request messages.

5. Provides access to the CDC for query purposes.
6. Two operating sites have been established, one at NCTAMS PAC, Honolulu, HI, and the other at NCTAMS LANT, Norfolk, VA. NCTAMS PAC will be designated as the Master DUSC (MDUSC) and NCTAMS LANT will be the Alternate DUSC (ADUSC). The MDUSC is the only site that will be allowed to provide update transactions for the UAC. The ADUSC will have the capability of assuming full DUSC responsibilities of the MDUSC for contingency purposes.

Commshifts are processed at the DUSC system. The DUSC system sends updates to the UAC (Update Authority Component). The UAC then updates the CDC (Central Directory Component). The CDC then updates/replicates information to all MSC's (Message Conversion System). The DUSC also sends commshift updates to the FSM and FMX sites.

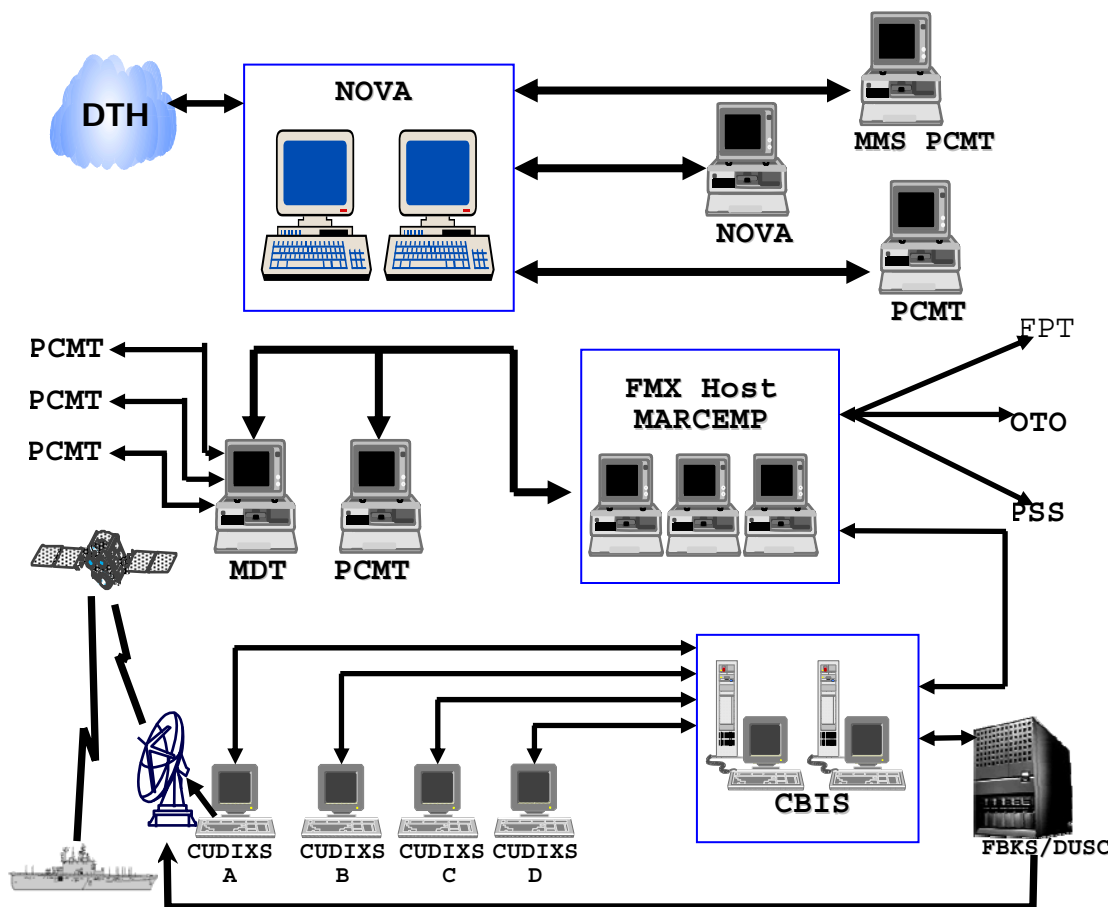


Figure 2-3  
FMX/DUSC configuration

### **2.2.8 FLEET SIPRNET MESSAGING (FSM)**

FSM is a point to point connection between the ship and the NOC. CUDIXS has become incapable of meeting the Navy's messaging needs. The use of NAVMACS II systems with IP connectivity has come to be the norm with reference to message traffic delivery. All units with IP capability equal to, or greater than, INMARSAT B HSD capabilities, are required to use FSM whenever possible. The end result is faster, more reliable record message traffic delivery to ships.

### **2.2.9 NEWSDEALER MSS and AMHS**

NEWSDEALER Message Switching System, much like the NOVA system, acts as the AUTODIN by-pass. NEWSDEALER MSS performs message switching, message safe storage, and message origination, creating a record communications infrastructure supporting the entire Intelligence Community. Both Defense Special Security Communications System (DSSCS) and General Service (GENSER) messages are exchanged. This system provides record communications for selected United States SIGINT System (USSS) field sites. Fielded systems have the capability to communicate with each other via the National Security Agency's wide area network (NSANet). Message routed outside of the USSS community are routed over the Defense Messaging Transition Hubs (DTH) or one of the NEWSDEALER Bridge Sites connecting NSANet and the Joint Worldwide Intelligence Communications System (JWICS).

Each NEWSDEALER is capable handling the ACP-128, DOI-103, DOI-103 Special format and Abbreviated Message Format (AMF). These systems may interface with computers, Automatic Message Handling System (AMHS), Message Correction System, Mode I and II circuits, STUIII Dial-up, and Virtual Circuit Protocol (VCP).

NEWSDEALER AMHS has simplified the task of drafting ACP, DOI 103, and DOI 103 Special formatted messages where as the actual message format is transparent to the user. AMHS provides simplified message drafting, coordination, and release of outgoing messages and a message internal distribution and delivery function for incoming messages.

A Virtual Circuit Protocol (VCP) has been defined to encapsulate record messages and transmit them using TCP/IP. As an added measure of security, a short header attached to the front of each VCP message transmitted contains a transaction ID indicating that it is a record message and the message size.

### **2.2.10 NAVAL MODULAR AUTOMATED COMMUNICATIONS SUBSYSTEM (NAVMACS)**

NAVMACS is designed to increase the speed, efficiency and capacity of naval afloat and ashore communications operations.

The NAVMACS modular concept allows the system to be configured according to the particular afloat platforms' requirements.

Current versions of NAVMACS are:

1. NAVMACS (V)2 provides up to four channels of fleet broadcast input; subscriber satellite interface to CUDIXS; and, the capability for on-line messaging. The (V)2 installation includes: computer (AN/UYK-20), teleprinter, printers, magnetic tape unit, paper tape unit and computer/satellite interface unit.
2. NAVMACS (V)3 offers more automated features for fleet users. The V3 program provides four channels of fleet broadcast input, four channels of Full Period Termination directly on-line with the system and a subscriber satellite interface to CUDIXS. NAVMACS V3 will support 2.4kbps NON-DAMA or DAMA operations via the CUDIXS link. The (V)3 installation includes: two computers (AN/UYK-20), video display units, printers, magnetic tape units, paper tape unit and computer/satellite interface unit.
3. NAVMACS (V)5 enhances automated communications with the addition of remote terminals for message input. The system also provides a subscriber satellite interface to CUDIXS. To allow drafters at remote locations as well as message center personnel the opportunity to edit and retrieve messages, storage is on disk in addition to magnetic tape. The (V)5 suite includes: three computers (AN/UYK-20A or AN/UYK-44), video display units, RD-433 disks, magnetic tape units, paper tape units, computer/satellite interface unit and printers.

(a) This system provides the operator with 24 flexible-purpose serial input/output (i/o) channels which can be configured as any of the following:

1. 75, 300, 600, 1200 baud circuits.
2. "Daisy-chained" remote displays and printers.
3. Remote systems, e.g., CVIC.
4. High speed tape readers.
5. High speed tape punches.
6. Compatible remote systems, e.g., Naval Intelligence Processing System (NIPS), and Personal Computer Remote System and (PCRS).

4. NAVMACS (V)5A like NAVMACS (V)5 also enhances automated communications with the addition of remote terminals for message input. This system was developed primarily for the AEGIS

equipped ships. The system also provides a subscriber satellite interface to CUDIXS. To allow drafters at remote locations as well as message center personnel the opportunity to edit and retrieve messages, storage is on disk in addition to magnetic tape. The (V)5A installation includes two AN/UYK-20A or AN/UYK-44 computers; three AN/USQ-69 video display units in the main communications space and up to eight more for remote message input/output; two RD-433 disks, for program loading and short term message storage; two AN/USH-26 cartridge magnetic tape units (CMTUs) for backup program loading and long term message storage; two RD-397/UG Paper tape units for message input/output; an ON-143(V) interconnecting box for interface between the computer and the satellite RF equipment; and three TT-624 high-speed printers located in main communications. It provides the operator with 14 flexible-purpose serial input/output (i/o) channels which can be configured as any of the following:

- a. 75 baud circuits.
- b. "Daisy-chained" remote displays and printers.
- c. External systems, e.g., CVIC.
- d. High or low speed tape readers.
- e. High or low speed tape punch
- f. Compatible remote systems, e.g., Naval Intelligence Processing System (NIPS), Personal Computer Remote System (PCRS)

5. NAVMACS II is a communications processor that provides message services to end users as well as command, control, and communications (C3) systems and will ultimately replace older versions of NAVMACS. It can be configured as either an afloat platform or as an ashore site. NAVMACS II replaces various communications systems previously employed by the U.S. Navy and all outdated versions of NAVMACS (V1 through V5/V5A). The purpose of NAVMACS II is to receive process, store, distribute, and transmit internal and external messages automatically. NAVMACS II provides interfaces to multiple external systems of the DMS, including land lines and radio frequency (RF) circuits. It also provides interfaces to local systems within the NAVMACS II network. NAVMACS II is supported by software that performs the communications processing required by all connected systems, including a user interface. It allows end users to perform a variety of tasks, based on their security clearance level, authorization, and need. Basic tasks include reading and sending messages to other users on site. Advanced tasks include configuring system databases and performing system administration (Figure 2-4).

NAVMACS II is configurable on a site-by-site basis for the unique requirements of its users. The system (designated AN/SYQ-7A(V))

architecture is based on the Tactical Advanced Computer-3 (TAC-3), a Hewlett-Packard™ 700 series computer. The minimum requirement for NAVMACS II is one TAC-3 computer (with the UNIX-based HP-UX™ operating system) configured as a "main communications" processor. The NAVMACS II main communications processor handles the processing and storage of all incoming and outgoing messages at a site, and is normally located in a site's primary communications area. Another type of processor may also be required in the main communications area to provide interfaces to external communication systems. This processor is the NAVMACS II Communications Controller (NCC). At sites with multiple users requiring access to NAVMACS II, additional TAC-3 computers may be configured as servers and clients on local area networks (LANs). Personal computers (PCs) may also be configured as clients.

The AN/SYQ-7B(V) configuration developed for smaller ships requiring less message throughput is similar to the above and executes the same software. This configuration uses the HP715 workstation. Only one NCC is configured with the system and a RAID disk subsystem is used instead of the second 1.2 Gb internal hard disk and the 1.02 Gb removable disk. The monitors of the HP715 are used instead of the X-Terminal. There is only one classified server in this configuration.

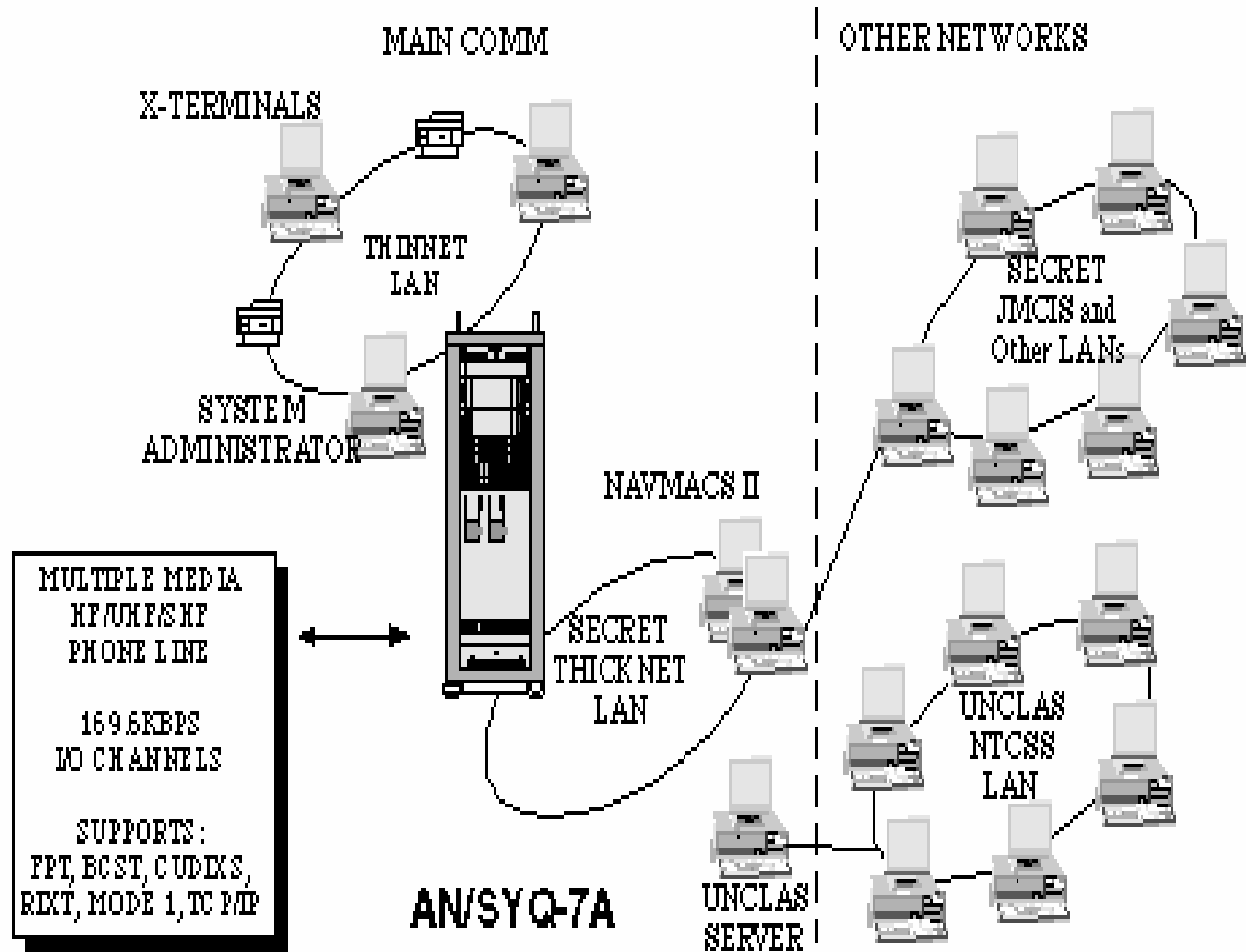
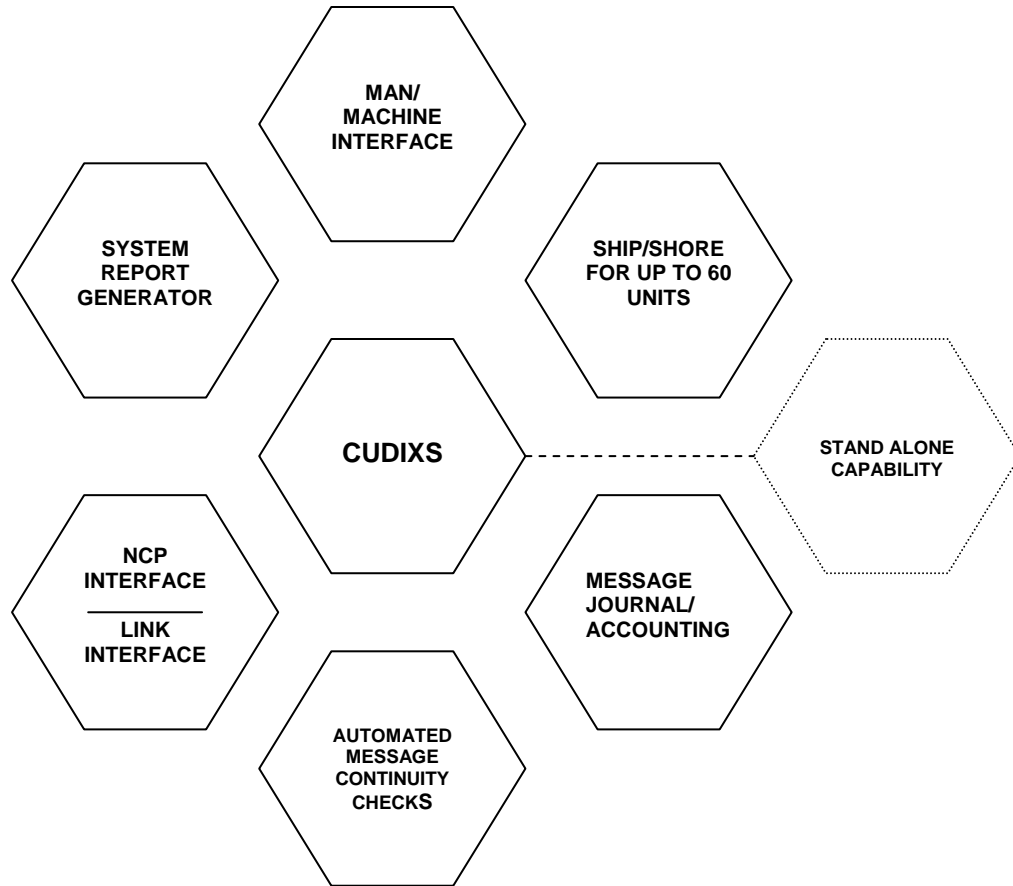


Figure 2-4  
NAVMACS II Configuration

2.2.11 COMMON USER DIGITAL INFORMATION EXCHANGE SUBSYSTEM (CUDIXS)

The two NCTAMS, NCTS GUAM, and NCTS Naples are equipped with CUDIXS. Figure 2-5 provides CUDIXS capabilities. Each site has at least three CUDIXS suites and the capability to operate two full and one "mini" configuration simultaneously. CUDIXS provides a 2400 baud full duplex interface, over a satellite link with mobile platforms, for the receipt and transmission of narrative message traffic between FMX and mobile platforms equipped with afloat automated systems. CUDIXS consists of the following hardware: computer (AN/UYK-20), video display unit, printer replacement program (PRP) computer, and computer/satellite interface unit. Up to sixty subscribers per CUDIXS suite have the capability to both send and receive narrative message traffic. Each subscriber can send and receive

Operator-to-Operator (OTO) orderwire type messages in free form and up to eighty characters in length.



**Figure 2-5  
CUDIXS Capabilities**

**2.2.12 SUBMARINE SATELLITE INFORMATION EXCHANGE SUBSYSTEM (SSIXS)**

The SSIXS provides the SSN/SSBN Commanding Officer with an optional satellite path to complement existing VLF/LF/HF broadcasts. When the position of the submarine permits visibility of a satellite, and where the tactical situation permits exposure of a submarine mast-mounted antenna, the subsystem provides rapid exchange of digital information between SSN/SSBN submarines and shore stations. It also provides access to the satellite path through a programmable mixture of query-



response and broadcast without query so as to provide maximum operational flexibility to the submarine commander. All transmissions provide automatic, reliable, long range, and cryptographically secure UHF communications between submarines and shore stations and submarines themselves.

SSIXS has the same equipment configuration as CUDIXS, except SSIXS uses magnetic tape for message storage. Additionally, the shipboard version of SSIXS has an ON-143(V)6 microprocessor for interface via satellite with the shore SSIXS.

### **2.2.13 BATTLE GROUP INFORMATION EXCHANGE SUBSYSTEM (BGIXS)**

Battle Group Information Exchange Subsystem (BGIXS) provides the BG Commander on a properly equipped CVN or LHA/LHD dedicated battle group additional SATCOM support.

The BGIXS provides capability for direct, two-way, tactical communication between deployed battle group units and submarines at 4800 or 9600 bps.

### **2.2.14 NAVY REGIONAL ENTERPRISE MESSAGE SYSTEM (NREMS)**

NREMS is the initiative to reduce the number of Navy DSP sites from five to two, eliminating the need for client-server DMS architecture and eliminating need for FORTEZZA cards / readers at the command desktop. NREMS provides web-based messaging capability that allows users (with accounts) to send and receive DMS messages using a web browser or via SMTP. The benefits are that it replaces current client-server DMS architecture and FORTEZZA at the command desktop and enables customers to use a personal computer web-browser to generate/receive messages and eliminate desktop software patches required by DMS.

NREMS provides DMS message service through the use of a web browser or SMTP e-mail client. Automated Message Handling System (AMHS) implements on-site redundancy and full Continuity of Operations Planning (COOP) capability between NCTAMS LANT and NCTAMS PAC. NREMS is scheduled to be complete in 2008.

## **2.3 FLEET BROADCASTS**

### **2.3.1 GENERAL INFORMATION**

With certain exceptions all ships, either individually or through guard ship arrangements will copy the Fleet Broadcast.

### **2.3.2 CONTROL OF THE FLEET BROADCASTS**

Control of the Fleet Broadcasts is the responsibility of the FLTCOM's and/or numbered Fleet Commanders and is accomplished by four distinctive components of the Fleet Broadcast Communications System. These four components consist of:

1. Broadcast Control Authority (BCA). The BCA implements an approved Fleet Broadcast, e.g., MULCAST, OPINTEL, RATT, for a specific communications area and provides direction and guidance to govern its assigned broadcast employment, configuration, and content. The responsibilities of a BCA may be self-assumed or delegated to a designated alternate.
2. Broadcast Control Station (BCS). The BCS provides all the technical aspects of affecting a Fleet Broadcast, which include assembling key streams received from the various Broadcast Keying Stations (BKS) into specific broadcast channels and delivering a composite key stream to the Broadcast Radiating Station (BRS) for transmission. BCS and BRS are normally integral parts of a NCTAMS. Stations that possess a TD-1150 and have connectivity to a particular BKS and BRS have the ability to perform BCS functions.
3. Broadcast Keying Station (BKS). The BKS introduces message or facsimile traffic into the Fleet Broadcast Network by generating a key stream of broadcast-bound information to the BCS for specific channel allocation before being forwarded to the BRS for broadcast transmission. Because of the diversity of broadcast-bound information, various BKS'S within the NAVCOMMAREA may key individual channels of multi-channel broadcast.
4. Broadcast Radiating Station (BRS). The BRS radiates the broadcast signal to the Fleet via Satellite, Super High Frequency (SHF), and/or Low Frequency (LF). Both area NCTAMS have the ability to rekey/radiate individual broadcast channels via 75BPS Guard Numbers on all DAMA networks upon approval from the numbered fleet commander controlling the broadcast. Additionally, those units that possess SHF terminations can receive individual broadcast channel support or receive the entire aggregate from area BCS via FCC-100 connectivity.

### **2.3.3 COMMUNICATIONS GUARD REQUIREMENTS**

Cognizant FLTCOM's require all commissioned ships and commands afloat to guard their assigned broadcast(s). Commands can meet this requirement by actively copying the broadcast or having the assigned broadcast screen ship in company supply the type channel of required broadcast. Only the vessels listed below are exempt from the above communications guard requirement:

1. Foreign manned MSC Ships (USNS).
2. Contract operated/tankers manned by civilians (USNS).
3. Time chartered ships under the operational control of MSC (SS).

4. Voyage chartered ships not under the operational control of the MSC, and cargo carrying ships at Berth (traffic rates).

With the advent of Automated Systems such as Fleet SIPRNET Messaging (FSM), SHF Gateguard units do not routinely submit COMSHIFTs when entering port. Units that do not resubmit COMMSHIFTs and lose primary delivery paths are cautioned that if primary path and secondary (ZOV path) are lost, Category I and II messages can and will be sent to tertiary paths listed in the latest COMMSHIFT on file at the Master Update Authority. For those units listing Fleet Broadcast channel (usually common channel) as an authorized ZOV route will have message traffic transmitted to it. Subsequently for those units not guarding the Fleet Broadcast while in port could possibly encounter numerous non-deliveries since the Fleet Broadcast does not require operator acknowledgement after the message is generated from the Fleet Message Exchange System (FMX). It is highly recommended that units that do not intend to monitor the Fleet Broadcast or CUDIXS termination while inport, have those ZOV routes removed from their COMSHIFT and replaced by a shore messaging system such as dial-in Gateguard or over the counter service to area NCTAMS.

#### **2.3.4 BROADCAST IDENTIFICATION**

Unique four-letter designators identify broadcasts. The first letter indicates the naval communication area (L-Atlantic and Mediterranean, P-Pacific). The second and subsequent letters identify whether it is a single or multiple channel broadcast and the broadcast type. NCTAMS LANT has assumed broadcast functions for the Atlantic and Mediterranean regions thusly removing the "M" designator that most communicators became familiar with. Additionally, NCTAMS PAC has conducted the same type merger for IMUL (Indian Ocean) Broadcast.

#### **2.3.5 FREQUENCIES**

Each NCTAMS generates Daily Communications Status Report Messages (often referred to as the 2301Z) that provide current down-link frequencies for UHF broadcast along with individual guard numbers for single channel DAMA support. In the rare event High Frequency (HF) support is required, submit Immediate precedence COMSPOT to the area NCTAMS to determine if single channel support is available in that area. HF, Multi-channel support is no longer offered to fleet units.

#### **2.3.6 CIRCUIT CONFIGURATION**

The source documents for block diagrams, equipment descriptions and quality control monitoring procedures for circuits are the Communications Quality Monitoring System documents (SPAWARSYSCOMINST 2700.1 and SPAWARSYSCOMINST C2700.2) dated 27 January 1989. Commands may order these documents from the ASO Naval Publications and Forms Center, 5801 Tabor Ave., Philadelphia, PA 19120-5099 using NSN 0913-LD-054-7770 and NSN

0691-LD-319-9600 respectively.

### **2.3.7 CRYPTOGRAPHIC COVERAGE**

Key list requirements and restart times for covered broadcast circuits are located in the appropriate CIBs; The EKMS Manager can provide the effective edition of the keying material. Restart procedures are per applicable CIBs and KAO'S. EKMS 1 (SERIES) contains information on cryptographic systems.

### **2.3.8 BROADCAST MESSAGE NUMBERING**

Each broadcast message is assigned a nine (9) position alphanumeric Broadcast Channel Sequence Number (BCSN) to ensure traffic continuity. The BCSN consists of a four-letter broadcast channel designator and a five digit sequence number, which indicates the number of cumulative transmissions that occurred for the particular channel. This number runs from 00001-99999 and is reset monthly at 010001Z. Should the sequence number exceed 99999 within a given month, the counter will reset to 00001 until the end of the month, and then reset again to 00001 to begin a new month. The BCSN is preceded by the message transmission identification (TI) indicator VZCZC (see paragraph below).

BCSN numbering continuity for overload channels is maintained the same way as above. In a situation where an overload channel is deactivated and then reactivated in the same month, the BCSN will run consecutively from the last number used. The overload channel activation message will indicate the first overload BCSN to be transmitted.

### **2.3.9 BROADCAST MESSAGE FORMAT**

Each message originally transmitted over a broadcast channel that is keyed by FBKS will be formatted as follows.

#### EXAMPLE

```
VZCZCPMAA01013
R 220933Z FEB 00 PSN 000207H09
FM JCS WASHINGTON DC
TO USS CHOSIN
INFO USS HUE CITY
USS GETTYSBURG
BT
UNCLAS //N02300//
MSGID/GENADMIN/JCS//
SUBJ/EXAMPLE OF A BROADCAST MESSAGE//
REF/A/GENADMIN/CHOSIN/101213ZFEB00//
RMKS/(40 MORE LINES OF TEXT)
PAGE 02 PMAA01013 UNCLAS
(REMAINING TEXT)//
BT
```

#01013  
NNNN

Each original broadcast transmission of a message, over either the single or multi-channel broadcast will begin with the Transmission Identification (TI) indicator and BCSN. The TI indicator consists of the characters "VZCZC". The V's purpose is to clear the circuit path of any extraneous characters and the ZCZC is to signal the start of a message indicated by the beginning of format line 2 of the message. Retransmissions will commence with the operating signal ZFG repeated three times.

EXAMPLE

ZFG ZFG ZFG  
VZCZCPMAA01014  
O 220514Z FEB 00 PSN 000472H13 ZNZ1  
FM USS SAN JOSE  
TO USS CALIFORNIA  
BT  
TEXT  
BT  
#01014  
NNNN

Before a message queues to a broadcast channel, FBKS validates delivery requirements specified in format lines 2, 4, 7 and 8. The system rejects misrouted messages to the DUSC for service action.

To save transmission time FBKS edits each message. Because format lines 2 and 4 are validated by Nova they are not transmitted. Side routes on format lines 7 and 8 are also validated and removed. Original page lines are removed and F/L 15 is replaced with the BCSN.

Lengthy messages are paged into blocks of 50 lines. Each page block will begin with a page number, BCSN, and the message classification. This is done to enhance a message's readability and ease of reproduction.

Nova assigns every message received an accountability number, called a Processing Sequence Number (PSN). This 6-digit number is included on F/L 5. It is followed by the site's letter identifier and a checksum of the PSN. The first letter of the BCSN and the F/L 5 site identifier will normally be the same. A difference between the two indicates that the screen action should be to the site identified on F/L 5.

Messages retransmitted over a single or multi-channel broadcast in reply to a Broadcast Screen Request (BSR) will begin with the operating signal ZDK repeated three times, followed by the TI indicator and the BCSN. The remainder of the transmission is the actual message beginning with F/L 5.

EXAMPLE

ZDK ZDK ZDK  
 VZCZC PMAA00036  
 R 162038Z FEB 00 PSN 017677H28  
 FM COMSPAWARSYSCOM WASHINGTON DC//PMW151//  
 TO USS ENTERPRISE  
 BT  
 UNCLAS //N02300//  
 MSGID/GENADMIN/CSWSC//  
 SUBJ/BROADCAST MESSAGE FORMAT//  
 RMKS/THIS IS AN EXAMPLE OF BROADCAST  
 MESSAGE FORMAT//  
 BT  
 #00036  
 NNNN

**2.3.10 BROADCAST RECAPS**

Every 30 minutes a message summary (RECAP) is transmitted for each active first-run and overload broadcast channel. The RECAP provides a summary of the traffic that was transmitted the previous half hour. RECAP'S are assigned immediate precedence and are queued at the top of the immediate message queue.

A RECAP message for a first-run channel will show the associated overload or rerun channel. Likewise, a RECAP for an overload channel will show the associated first-run channel. Shipboard personnel should note this information each time a RECAP is received. This will help insure all appropriate broadcast channels are being copied.

The text of the RECAP reflects the BCSN, precedence, date-time-group, originator and broadcast addressees for each message transmitted on that broadcast channel. RECAP DTGs are always assigned on the half hour. Part one identifies the message transmitted including precedence, DTG, Originator, and any pertinent Q and Z signals. Part two identifies the specific CSNS that were sent to specific commands. The following depicts the format of a RECAP for the Pacific Overload Broadcast.

EXAMPLE

VZCZCIOCC01019  
 O 230200Z FEB 00 ZNZ  
 FM FMX PAC HONOLULU HI  
 TO POCC BCST  
 BT  
 UNCLAS SVC //N00000//  
 SUBJ: BROADCAST RECAO 230130 FEB 07 - 210200 FEB 07  
 POCC OVERLOAD - PMCC FIRST RUN  
 PART ONE  
 01013 R 220933Z JCS WASHINGTON DC/USS CHOSIN/USS HUE CITY

01014 0 220514Z USS SAN JOSE/USS CALIFORNIA/ZNZ  
 01015 P 201514Z COMNAVNETOPSCOM WASHINGTON DC/CTF FOUR TWO  
 01016 P 230005Z FLEWEACEN GUAM/ZPW 240001Z FEB00  
 01017 R 230105Z USS SAN FRANCISCO/COMTHIRDFLT/  
 01018 CANTRAN  
 PART 2  
 PMCC BCST  
 01013 01015 01016  
 USS CHOSIN  
 01014  
 CTF FOUR TWO  
 01017  
 BT  
 #01019  
 NNNN

### 2.3.11 BROADCAST SERVICE MESSAGES

#### Broadcast Screen Request (BSR)

BSR is a PROFORMA message designed for fleet broadcast subscribers to request the transmission (ZDK) of messages missed or received garbled on any fleet broadcast. PROFORMA messages should be prepared using the approved message preparation software program. Every message sent over a broadcast channel is retransmitted over the associated rerun channel after a two-hour delay, if the rerun channel is not being used for some other purpose. Broadcast Keying Stations (BKS) generate summary messages every half-hour identifying intended recipients of a particular broadcast number. This helps recipients identify missing broadcast numbers/messages. Prior to sending a BSR to the broadcast station, every attempt must be made to obtain the missed messages from rerun channels, ships in company while underway, or shore communications facilities when in port. Subscribers will ensure each BSR cancels previous outstanding requests and lists all outstanding numbers on the broadcast channel concerned. Ships will send BSR's to the BKS unless otherwise directed.

If a recipient misses 50 or more broadcast numbers, the numbered fleet commander shall be included as an information addressee and a reason for outage should be identified by adding a remarks set to the BSR PROFORMA message. If the request is in excess of 100 total broadcast numbers, separate BSR'S in increments of 50 numbers must be generated. BSR's received with more than 100 Broadcast Screen Numbers (BCSN) will be rejected.

Each BSR will be complete in itself and will include all numbers missing at the time of submission, less missed numbers known not to be addressed to ship's or embarked commander's guard list. This information is available on hourly FMX generated RECAP summary messages.

Embarked commanders who are assigned a routing indicator (RI) different from the RI assigned to the host ship must be included

when submitting a BSR. Embarked commanders, squadrons, detachments, etc., which share the host ship's or embarked commander's RI will not be included.

If a Broadcast Screen Ship (BSS) is designated prior to an exercise or operation, the BSS is responsible for gathering missed message input for ships in company and submitting a consolidated BSR.

The following format is currently used for submission of BSR'S. Detailed information for drafting BSR'S is available in NTP 4 Supp-2.

Retransmissions in response to BSR'S are only provided to those ships which are addressees (or have embarked commands) addressed in the missing numbers (messages) requested. Retransmissions are transmitted under the original broadcast numbers prefixed with a ZDK pilot.

In the event of an FMX failure which causes the BKS functions to be shifted, instructions will be provided to fleet units concerning BSR submission procedures.

EXAMPLE

```
RTTUNJSR RUEOMID3463 1191000-UUUU--RHMCSUU.
ZNR UUUUU
R 281000Z APR 00 ZYB
FM USS JOHN C STENNIS
TO FMX PAC HONOLULU HI
BT
UNCLAS //N02790//
MSGID/BSR/STENNIS//
SCRN/USS JOHN C STENNIS /COMCARGRU THREE//
CHAN/PMMA/BSN:00012/BSN:00023/BSN:00050/BSN:00053//
CHAN/PMCC/BSN:00056/BSN:00087//
SCRN/ATKRON FIVE FOUR TWO//
CHAN/PMDD/BSN:00090/BSN:00092/BAND:00100-00103/BSN:00113//
SCRN/USS JOHN C STENNIS //
CHAN/PMCC/BSN:00075//
PERIOD/200001ZJAN2001/242359ZJAN2001//
BT
#3463
NNNN
```

Broadcast Screen Summary (BSS)

The FBKS in response to a BSR generates the Broadcast Screen Summary (BSS). The BSR response will originate from the servicing FMX site and will bear the appropriate PLA for the site, i.e. FMX PAC HONOLULU HI. Examples of BSS responses are listed below:

1. NO MESSAGES FOUND. (MASTER UPDATE AUTHORITY has screened originator BSR and missing messages are of no concern to



- originator.)
2. FOL NRS CANTRAN.
  3. FOL NRS ZFK 1/2.
  4. FOL NRS ZDK AT TIMES INDICATED.
  5. FOL NRS ZDK ASAP.
  6. FOL NRS ZOV ASAP.
  7. FOL NRS TO BE TRANS WITH NEW NRS.
  8. FOL NRS TRANS AT TIMES INDICATED.
  9. ERROR. (BSR contains error(s), Unable to process correct and resubmit.)

#### Broadcast Screen Summary Reply Example

```

OTTUZYUW RHOENPM0099 0311030-UUUU--RHMCSUU.
ZNR UUUUU
O 311030Z JAN 00 ZYB
FM FMX PAC HONOLULU HI
TO USS NIMITZ
BT
UNCLAS
MSGID/GENADMIN/FMX PAC//
SUBJ/BROADCAST SCREEN SUMMARY//
REF/A/BSR/NIMITZ/311000ZJAN2001/-/NOTAL//
RMKS/
1. ATKRON FOUR TWO
A. NO MESSAGES FOUND.
2. USS NIMITZ
A. FOL NRS CANTRAN: PMAA00023.
B. FOL NRS ZFK 1/2 : NONE.
C. FOL NRS ZDK AT TIMES INDICATED: PMAA00012/0310930.
D. FOL NRS ZDK ASAP: PMAA00050, PMAA00053, PMCC00053, PMCC00087.
3. USS JOHN C STENNIS
A. FOL NRS ZOV/ASAP: PMCC00075
4. ERROR/USS NIMITZ/CHAN/PMDD/FIELD 5 INVALID, 99003 - UNABLE TO
PROCESS/CORRECT AND RESUBMIT//
BT
#0099
NNNN

```

Figure 3-3 is the check-off sheet used for keeping a record of broadcast numbers received or transmitted. This form provides for the number received, the classification of the message, and also provides a record of destruction for classified traffic. These forms may be reproduced locally. A similar form is available through supply channels (Stock number 0196-LF-301-8350).

### 2.3.12 BROADCAST OFF THE AIR MONITORING (OTAM)

OTAM is a computer-based monitoring system for up to 16 circuits. The fleet centers located at the NCTAMS and selected NAVCOMTELSTA'S monitor the fleet broadcast by receiving the same broadcast copied by fleet units. The monitor copy ensures channel continuity, crypto synchronization, and provides an analytical source for identifying and solving problems.

All broadcast channels transmitting live traffic (including those uncovered) will be monitored off the air to ensure proper operation. Area NCTAMS may assign OTAM responsibilities for individual broadcast channels to stations other than the originating station provided the designated stations can meet the tasking within existing manpower and equipment resources. No more than one station is required to monitor the same broadcast channel except when unusual conditions dictate. Keep NETWARCOM advised of situations involving unusual conditions. Support and residual stations which rekey broadcasts are required to conduct normal quality control of broadcast circuits and where equipment allows, should spot check with OTAM as part of the quality control effort.

Include the term OTAM in the remarks column of the broadcast line item in the station TELCOR Section I summary. Broadcast originating stations and those commands assigned OTAM functions are to include the broadcast monitoring and broadcast transmit equipment in the appropriate sections of the communications operating facility report.

## 2.4 TYPES OF BROADCASTS

### 2.4.1 FLEET MULTICHANNEL BROADCAST SYSTEM

The Fleet Multi-channel Broadcast System (MULCAST), provides the means of delivering message traffic to the Fleet. The MULCAST System is a highly flexible system providing global broadcast service to the Fleet via four major communications areas. FBKS keys the MULCAST. The paragraphs below describe the characteristics of MULCAST in terms of its broadcast area, FLTCOMS, operating frequencies, channelization and general operating procedures.

#### BROADCAST AREA FLTCOM

HMUL/PMUL	PAC	COMTHIRDFLT/COMSEVENTHFLT/ COMPACFLT
LMUL	LANT	COMSECONDFLT/COMUSFLTFORCOM COMSIXTHFLT/COMUSNAVEUR

Operating frequencies: MULCAST may be operated on Satellite, Low Frequency (LF), Medium Frequency (MF), High Frequency (HF) and

Ultra High Frequency (UHF) ranges. Consult current CIB'S for operating frequencies.

Due to inherent limitations of HF propagation, the HF component of the MULCAST (when activated) is transmitted simultaneously on several frequencies to permit diversity reception. In some cases, diversity reception overcomes the anomalies of HF propagation and reduces the probability of broadcast interruption. Recipients of the MULCAST can use one of two methods for diversity reception which are:

Frequency of RF diversity in which the information signal is transmitted/received on two separate frequencies simultaneously. Shipboard use of frequency diversity permits uninterrupted circuit operation since fading over two different frequencies will seldom occur at the same time. Polarity diversity uses a vertically and horizontally polarized antenna to copy a single frequency.

A maximum of sixteen channels of information are combined to form the multi-channel broadcast. The multi-channel broadcast transmitted via satellite carries 15 channels of information (channel 16 contains system frame/sync data). Most ships maintaining their own guard are required to copy at least the common channel. If traffic tempo dictates, overload channels are activated to clear first run traffic. When required, overload channels are also used to rekey allied broadcasts in support of U.S. units participating in combined operations. Area CIB's reflect the current assignment of broadcast channels. These broadcasts are normally keyed continuously but require restarts at the beginning of each new CRYPTO day.

Normally all first-run traffic is retransmitted two hours later over the associated rerun channel, i.e., PMAA first-run traffic sent between 1400Z-1500Z will be transmitted over the rerun channel PRAA at 1600-1700Z. Because this procedure allows communications personnel the opportunity to copy broadcast numbers missed during the first transmission, submitting Broadcast Screen Requests (BSR) to obtain lower precedence missed numbers should be delayed until after the rerun transmission (see paragraph 419). If a RECAP message indicates that the missed number (message) is addressed to your ship/unit and the precedence is immediate or higher, BSR action may be necessary sooner.

Once a queue has been depleted on a first-run channel, it and its associated overload channel (if assigned) will commence rerunning messages. The last message transmitted will be the first message rerun. For example, if LMAA01016 was the last message transmitted it would be the first message rerun, followed by LMAA01015, LMAA01014, etc. A channel will revert to a first-run status whenever a new message is received.

#### **2.4.2 WORLD-WIDE TACAMO (WTAC)**

TACAMO (Take Charge And Move Out) is a survivable communications link during trans-attack and post-attack phases of conflict. It enables the President and the Secretary of Defense to directly contact submarines, bombers and missile platforms protecting our national security through strategic nuclear deterrence.

#### **2.4.3 USW PATROL (VP) BROADCAST**

The nature of USW patrol (VP) aircraft operations requires dedicated transmission of all ground-to-air traffic using the broadcast method. The VP broadcast operating in the HF mode serves as the primary vehicle for delivery of operational messages to aircraft regardless of the aircraft's mission, emission mode or supplemental means for delivery. COMPATWINGSPACINST C2330.1 and the Consolidated Maritime Brief Book provide broadcast operating instructions for the Pacific and Atlantic Ocean areas respectively.

#### **2.4.4 SCI FLEET BROADCASTS**

SCI communications utilizes three broadcasts, LMFF, IMNN and PMFF for the sole purpose of providing Over the Air Transfers (OTATs) of COMSEC keying material. These broadcasts are included in each particular fleet area, SSR-1 provided broadcast. Weekly OTATs are issued by UARNOC on the 7<sup>th</sup>, 14<sup>th</sup>, 21<sup>st</sup>, 28<sup>th</sup> and last day of the month. OTAT messages are sent the day prior to transmission of the OTAT. The OTAT message will contain the listing of the keying material that will be transmitted and the time of transmission.

### **2.5 MANAGEMENT AND CONTROL SYSTEMS**

#### **2.5.1 AUTOMATED DIGITAL NETWORKING SYSTEM (ADNS)**

The primary function of the ADNS is to connect Navy shipboard networks to other ship and shore networks for transferring Internet Protocol (IP) data of various classification levels. The shipboard user can connect to the external networks of other Navy platforms and facilities and the Wide Area Networks (WANs) provided by the Defense Information Systems Agency (DISA). The ADNS system is designed to allow network enclaves to route (IP) data over multiple RF mediums. The RF services include, but are not limited to, Super High Frequency Defense Satellite Communications System (SHF DSCS), Extremely High Frequency/Medium Data Rate (EHF/MDR), Extremely High Frequency/Time Division Multiple Access (EHF/TDMA) Interface Processor (EHF/TIP), International Marine/Maritime Satellite (INMARSAT B), SHF Commercial Wideband SATCOM program (CWSP) (which will be replaced by the Commercial Broadband Satellite Program (CBSP) beginning in 2008) and pier connections. The ADNS system provides Wide Area Network (WAN) connectivity to the shore by passing IP data over available RF mediums using Point-to-Point Protocol (PPP) for link establishment and maintenance. By dynamically routing IP data using Open Shortest Path First (OSPF), the ADNS system can choose

which RF link to use to reach the shore.

### **2.5.2 RADIO COMMUNICATIONS SYSTEM (RCS)**

The Radio Communications System (RCS) consists of several exterior communications subsystems which, in combination, provide all exterior communications requirements for the ship with the exception of the Special Intelligence Communications requirements. The RCS subsystems are turnkey installations and consist of the following subsystems: High Frequency Communications System, Very High Frequency Communications System, Ultra High Frequency Line-of-Sight Communications System, Ultra High Frequency Satellite Communications System, Extremely High Frequency Satellite Communications System, Super High Frequency Satellite Communications System, Communications Support Segment, Naval Modular Automate Communications System II, and the Bridge to Bridge Communications System.

### **2.5.3 NAVY ORDERWIRE TERMINAL (NOW)**

NOW is A PC-based system that supports up to four full duplex circuits using Navy Orderwire software in conjunction with two Frontier Communications boards. The system replaces Teletype equipment formerly used on four orderwires and has message storage and retrieval capabilities as well as an editor for message preparation. Circuit logs may also be stored and retrieved. An optional printer may be attached for message copies and logs. This circuit is not certified and will not be used to pass traffic except as a last resort.

### **2.5.4 AUTOMATED NETWORK CONTROL CENTER / AUTOMATED TECHNICAL CONTROL (ANCC/ATC)**

The ANCC and ATC are functionally identical except for size. ANCC/ATC replaces manual patch and test facilities ashore with a fully redundant computer-controlled switching and circuit monitoring system. This system provides the ability to reconfigure equipment interconnectivity and perform circuit monitoring for out-of-tolerance conditions in advance of circuit outages. At deployed locations, this system supplies 98 percent of voice, video, and data connectivity. Failures result in major C4I disruption of services to and from the operating forces in an entire communications area.

### **2.5.5 MULTI-CIRCUIT PATCH PANEL (MCP)**

The multi-circuit patch module provides for equipment interfaces requiring a database (DB)-type interface. It contains two non-powered (without LEDs) multi-circuit patch panels and a quick connect panel QCP. Two of the patch panels contain 17 patch modules while the others contain 16 patch modules. The two containing 17 patch modules have a test module with a DB 25-pin connector and standard modular patch jack. The two containing 16

patch modules have a test breakout module for connecting individual signals. Each patch module has line, equipment, and monitor appearances. The common signal interface to a patch module will be electronic industry association (EIA) standard RS-232 for unbalanced and RS-530 for balanced. However, the following common interfaces RS-232/-423/-422/-530 or MIL-STD-188-114 can be accommodated. Up to eight RS-423/-422 37-pin interfaces and twelve RS-232/-530 25-pin interfaces can be selectively pinned out using the QCP, thus eliminating a need to fabricate special cables when deployed. Interfaces from the multi-circuit module may also be routed through the high-speed COMSEC case for encryption/decryption. Two multi-circuit modules are provided with each TCTC package.

All Transit Case Technical Control (TCTC) modules may be interconnected using one-for-one standard DB 25- or 37-pin connector cables available from most telecommunications companies. Depending on the TCTC module, a number of female connectors on a rear signal entrance panel (SEP) are available for interfacing between modules. This allows interfacing with equipment using one-for-one cables to facilitate rapid set-up and interface. Connectors on the module SEPs are identified by the signal interface convention to which they conform; i.e., RS-232/423/422/530 and MIL-STD-188-114. To accommodate equipment-specific pin-outs, signal conversions are accomplished in the TCTC module using quick connect/disconnect panels, thus eliminating the need to fabricate special cables when deployed. CJCSM 6231.01B defines the joint communications network model that the TCTC supports. A deployed JTF in a bare-base environment provides the basis for this model. The model can be changed to meet specific operational requirements. Internodal communications provides connectivity among DISN, JTF headquarters, and service component headquarters and their forces, along with supporting elements such as the JSOTF and its subordinate forces. The Air Force, Army, Navy, and Marines have component headquarters and forces. This network links the deployed locations by satellite and microwave troposcatter/line of sight. This transmission media supports the extension of common-user transports consisting of JWICS, NIPRNET, SIPRNET, record communications (AUTODIN and DMS), VTC, and other special-purpose circuits. The TCTC is capable of extending all of these transports or communication services.

#### **2.5.6 SA2112 (V) (SAS)**

The heart of the radio transmitter and receiver distribution system is the SA-2112 single audio system (SAS). The SA-2112 secure switching unit, commonly referred to as the SVS or "coke machine", is the key element in the SAS. The SAS provides the ship with an integrated secure (cipher)/nonsecure (plain) R/T voice system. SAS features allow remote operating positions to select either cipher or plain voice operations without reconfiguring the existing system. It also provides automatic switching between remote operating positions and radio sets or

crypto equipment, centralized control and monitoring of the system, and a built-in-test (BIT) capability.

#### **2.5.7 TIMEPLEX LINK 2+**

The LINK/2+ has become the primary full or half-duplex, first level multiplexer for Navy tactical SHF communications. LINK/2+ is an intelligent transmission resource manager (TRM) currently supporting Navy SHF and commercial operations, providing high-performance networking capabilities for facilities with large I/O requirements. It is a multi-system high-capacity networking device for voice, data, and imagery communications transmissions over T-1/2.048 Mbps data rate (European) (E1) or lower speed facilities. It provides smart multiplexing, bandwidth efficient management and full network management capabilities.

The LINK/2+ incorporates a modular design for enhanced flexibility, reliability, and improved network performance. Navy SHF uses a basic 18-slot chassis, with the capability of an 18-slot-expansion chassis (two-nested) system. It is capable of processing digital data, voice (voice compression), and video synchronous, asynchronous, isochronous, asymmetrical (different transmit and receive speeds on the same channel), and simplex signal processing.

The LINK/2+ is capable of operating 12 trunks at aggregate data rates of 4.8 Kbps to 2.048 Mbps each (not to exceed 7 T-1's, each at 1.544 Mbps).

### **2.6 NETWORK SERVICES AND ARCHITECTURE**

#### **2.6.1 ROUTING ARCHITECTURE**

Routing involves the forwarding of IP packets across a network to the intended destination IP address. Routing occurs at Layer 3 (the network layer) of the OSI reference model. To determine the optimal path for a packet to travel, routing protocols use metrics. To assist the process of determining the path a packet will travel, routing algorithms create and maintain routing tables (list of associations used to decide the next router a packet should be sent to reach ultimate its destination).

#### **2.6.2 DISN TRANSPORT SERVICES**

The Defense Information System Network (DISN) provides a variety of voice, video and data transport services for classified and unclassified users in the continental United States (CONUS) and overseas (OCONUS). DISN supports customer requirements from 2.4 Kbps to 155 Mbps (OCONUS) and 2.5 Gbps (CONUS). Its best-value network solutions include inherent joint interoperability, assured security, redundancy, high reliability/availability, 24/7 in-band and out-of-band network management, engineering support and customer service.

DISN transport services are available to all Department of Defense (DoD) agencies and military services, as well as other federal government agencies. Services can be ordered through the telecommunications control officer (TCO), who will validate requirements and verify funding authorization.

### **DoD Teleport System**

The Defense Information Systems Agency (DISA) is implementing the Department of Defense (DoD) Teleport System. The system will integrate, manage, and control a variety of communications interfaces between the Defense Information System Network (DISN) terrestrial and tactical satellite communications (SATCOM) assets at a single point of presence.

The system is a telecommunications collection and distribution point, providing deployed warfighters with multiband, multimedia, and worldwide reach-back capabilities to DISN that far exceed current capabilities. Teleport is an extension of the Standardized Tactical Entry Point (STEP) program, which currently provides reach-back for deployed warfighters via the Defense Satellite Communications System (DSCS) X-band satellites. This new system provides additional connectivity via multiple military and commercial SATCOM systems, and it provides a seamless interface into the DISN. The system provides inter- and intra-theater communications through a variety of SATCOM choices and increased DISN access capabilities.

The system will be implemented in three phases:

1. Generation One - Currently being implemented. Generation One (FY02-08) architecture adds capabilities to a subset of existing STEP sites. It will provide satellite connectivity for deployed tactical communications systems operating in X-band (DSCS and follow-on X-band satellites), commercial C- and Ku-bands, Ultra High Frequency (UHF), Extremely High Frequency (EHF) SATCOM and initial Ka-band capabilities.

2. Generation Two - This generation (FY 06-08) consists of implementing additional Ka-band terminals and a NETCENTRIC capability. The Ka-band terminals will provide interfaces to the Wideband Global System (WGS) program, which will provide Ka-band and X-band coverage with throughput far exceeding the current DSCS satellite constellation.

3. Generation Three - This Generation is currently undefined and funding has not been identified. A capabilities development document is in development and a funding approach will be sought by the Joint Capabilities Board. For more information **Email:** [dodteleport@disa.mil](mailto:dodteleport@disa.mil).



## **GIG Enterprise Services**

The Defense Information Systems Agency's (DISA) Global Information Grid Enterprise Services Engineering (GE) directorate plans, engineers, acquires and integrates joint, interoperable, secure global net-centric solutions satisfying the needs of the warfighter and develops and maintains a first-class engineering workforce to support the needs of DISA's programs. GE's core competencies include disciplined IT end-to-end systems engineering, security expertise for the Global Information Grid, leveraging commercial-off-the shelf products and services to solve joint and coalition needs and provide value added, trustworthy global net-centric solutions. Contact: GES Project Office at [ges@disa.mil](mailto:ges@disa.mil).

## **Global Combat Support System (GCSS) Combatant Commanders/ Joint Task Force (CC/JTF)**

GCSS (CC/JTF) is an initiative that provides end-to-end visibility of retail and unit level Combat Support (CS) capability up through National Strategic Level, facilitating information interoperability across and between CS and Command and Control functions. In conjunction with other Global Information Grid elements including Global Command and Control System-Joint, Defense Information Systems Network, Defense Message System, Computing Services, and Combatant Commands/Services/Agencies information architectures, GCSS (CC/JTF) will provide the information technology capabilities required to move and sustain joint forces throughout the spectrum of military operations.

GCSS (CC/JTF) supports the Combatant Commanders and their assigned Joint Task Forces by providing access to comprehensive logistics information from authoritative data sources. This access provides the warfighter with a single, end-to-end capability to manage and monitor units, personnel and equipment through all stages of the mobilization process. By providing access to high-level integrated information, GCSS (CC/JTF) enhances the ability of Combatant Command and JTF Commanders to make timely, informed decisions based on the near real-time or predicted status of his resources.

## **Mission**

Provide end-to-end information interoperability across combat support and command and control functions to support the Combatant Command & Joint Task Force Commanders.

## **GCSS (CC/JTF) Warfighting Capabilities**

1. Provides dynamic access to command & control, intelligence, and logistics data via a single gateway.

2. Provides browser-based, PKI-enabled capabilities on the SIPRNet and CAC-enabled capabilities on the NIPRNet.
3. Provides joint logistics applications via a single sign on.
4. Single, Mobility System, Global Transportation, Network, Intelligent Rail/Road Information Server, Asset Visibility, In-transit Visibility, Integrated Data Environment.
5. Consuming web services from NGA's mapping capability (Adopt before you buy, Buy before you Create).
6. Provides access to NCES' E-Collab from GCSS (CC/JTF).
7. Provides permission-based, knowledge management system (KMS) for file-sharing within and across combatant commands.
8. Provides ability for end-users to run reports and export to other formats, e.g., briefing, spreadsheet, .pdf.
9. Provides a Watch Board to monitor critical items.
10. Provides a modular, net-centric, service oriented environment for agile, flexible, rapid development and delivery of critical capability.
11. Provides a Civil Engineers Modeling tool: Joint Engineering Planning and Execution System (JEPES).

### **2.6.3 COMMUNICATIONS WITHIN DISN DATA SERVICES NETWORKS**

#### **CONNECTIONS TO THE INTERNET**

1. All bureaus and posts having access to OpenNet are required to establish Internet connectivity through OpenNet Plus. If OpenNet service is available to the bureau/post, the Department will no longer fund or approve Dedicated Internet Network (DIN) service unless the bureau or post has a valid waiver to implement a DIN.
2. A post may have a contract with an Internet Service Provider (ISP) to provide bandwidth for contingency and VNet (also know as Virtual Private Network (VPN)) provided and managed by IRM/OPS/ENM/ND. This is to provide the post with an alternate route for connectivity back to the Open Net infrastructure and does not require a waiver.
3. Information Resource Center (IRC) public access terminals have been granted a waiver from this policy; i.e., ODI (Overseas Dedicated Internet) LANs may continue to provide Internet access and other Public Diplomacy services to the public. Local networks used as test, development, web hosting, and research environments may also connect locally to the Internet, but can only do so after receiving a waiver. These Local Area Networks (LANs) are not to be linked to

OpenNet Plus or used by employees to carry out Department business transactions. Bureau/post must terminate all unauthorized use of ODI LANs no later than 90 days after OpenNet Plus is implemented at the bureau/post.

4. The Department realizes that there may be exceptions to the requirement for accessing the Internet via the OpenNet. Posts and bureaus may request a waiver to this policy. The IT Change Control Board (CCB) will review such requests on a case-by-case basis.

#### **REQUESTING A WAIVER TO THE INTERNET CONNECTION POLICY**

A Bureau/post requesting authorized continued use of a Dedicated Internet Network (DIN) connection must submit the DIN access waiver request. All DIN solutions must comply with the Department's standards and FAM guidance. Provide the following information when submitting the waiver request:

1. Post or bureau name.
2. Post or bureau point of contact, e-mail address, and telephone number.
3. Location serviced by DIN.
4. Type of Internet access service (DSL, dial-up, other).
5. Configuration details (number of connections, users, rooms to be served).
6. Purpose of the service.
7. Reason requirement cannot be satisfied through OpenNet Plus (for example: Protocol is not available through OpenNet Plus—website not accessible).
8. What post/bureau is doing to reduce risks (i.e. firewalls, virus protection).
9. Projected costs.
10. Timeframe of exception.

Submit DIN Access Waiver Requests by e-mail to "IT CCB Management" or by telegram or memorandum to the IT CCB Change Manager, IRM/OPS/ENM/NLM/ECM. The IT CCB Change Manager will conduct an abbreviated review with relevant IT CCB primary review authorities and will ensure the request appears on the next IT CCB meeting agenda for consideration and decision.

If a request for a waiver is denied, the bureau/post may send an appeal to the Chief Information Officer for final decision. If a bureau/post's network is connected to the Internet outside of OpenNet Plus and without the signed DIN waiver, the bureau/post is in conflict with security guidelines. If unauthorized Internet connections are detected, the responsible office will be instructed to disconnect them.

#### **2.6.4 SWITCHES AND ROUTERS**

A network switch is a computer networking device that connects network segments. Low-end network switches appear nearly identical to network hubs, but a switch contains more "intelligence" (and a slightly higher price tag) than a network hub. Network switches are capable of inspecting data packets as they are received, determining the source and destination device of that packet, and forwarding it appropriately by delivering each message only to the connected device it was intended for, a network switch conserves network bandwidth and offers generally better performance than a hub.

A router is a device that extracts the destination of a packet it receives, selects the best path to that destination, and forwards data packets to the next device along this path. They connect networks together; a LAN or WAN for example, to access the Internet. Some routers are available in both wired and wireless models.

#### **2.6.5 UNCLASSIFIED BUT SENSITIVE INTERNET PROTOCOL NETWORK (NIPRNET)**

NIPRNET is a global long-haul IP based network to support unclassified IP data communications services for combat support applications to the Department of Defense (DoD), Joint Chiefs of Staff (JS), Military Departments (MILDEPS), and Combatant Commands (COCOM). Provide seamless interoperability IP services to customers with access data rates ranging from 56Kbps to 1.0Gbps via direct connections to a NIPRNET router, remote dial-up services (56Kbps), services to the Tactical community via ITSDN/STEP sites, and access to the Internet.

#### **2.6.6 SECRET INTERNET PROTOCOL NETWORK (SIPRNET)**

SIPRNET is the DoD's largest interoperable command and control data network, supporting the Global Command and Control System (GCCS), the Defense Message System (DMS), collaborative planning and numerous other classified warfighter applications. Direct connection data rates range from 56Kbps to 155Mbps. Remote dial-up services are available to 19.2Kbps.

#### **2.6.7 AUTHORIZED SERVICE INTERRUPTION (ASI)**

DISA policy requires that the best possible communications service be provided to warfighters and users of the Global Information Grid (GIG). This correlates to the availability of communications equipment and facilities. Periodic maintenance varies from the removal of equipment to a complete shutdown of a

DISN facility. These scheduled interruptions are generally known in advance and every effort must be initiated to provide continuity of service to the users during the scheduled interruptions. The DISA CONUS ASI Manager is the approval authority for routine service interruption requests on DISN stations, nodes, links, trunks, and circuits. The DISA CONUS Commander is the sole authority for approving/canceling ASIs with the CONUS Theatre. Cancellations and rescheduling will be accomplished by the DISA CONUS ASI Manager in conjunction with the guidance provided by the DISA CONUS Commander in coordination with the Global NetOps Center (GNC).

**Types of ASIs:**

Emergency Service Interruption (Real time operational impact only): Service interruptions to correct hazardous or degraded conditions where loss of life/property could occur through lack of immediate action. No prior coordination or user release is required (reference DISA Circular 310-70-1, c7.3.4.7). The facilities involved must notify users when time permits and report the circumstances to the NOC Controller or SCO/Watch Officer as soon as possible. These situations must also be reported to the appropriate DISA and O&M elements as time permits.

**Urgent Service Interruptions:**

Service interruptions that do not qualify as an emergency but are requested inside the 21-day prior notice period. A justification to waive the 21-day prior notice requirement must accompany the initial request. The DISA CONUS ASI Manager will stringently review the request and justification. The only exception to the 21-day notice policy is for the P4035 Optical contractor.

NOTE: Lack of coordination or resources is not a valid justification. It is important to note that urgent requests that do not have a valid 21-day justification will be handled as routine requests. The Commander, DISA CONUS has sole authority to approve urgent ASIs once customer concurrence is received.

**Routine Request:**

A service interruption in which the request is received no later than 21 days prior to the requested scheduled interruption. The requesting O&M elements must notify the DISA CONUS ASI manager no later than 21 days in advance of the requirement and request tentative approval. The only exception to the 21-day notice policy is for the P4035 Optical contractor. Facilities must submit times/dates avoiding peak traffic hours (1100z - 1800z) during the weekday. However, if a CONUS ASI will affect a real time mission in another AOR, the ASI will be scheduled to accommodate that mission.

Upon completion of the ASI, the appropriate maintenance activity will notify the NOC Controller or SCO/Watch Officer. The GNCS SCO will provide verbal notification to the GNC SCO of the ASI status.

Extension of an Ongoing Approved ASI - The GNC has sole authority to approve/disapprove ASI extensions for inter-theater systems supporting Europe, Pacific, and CENTCOM arenas. The GNSC SCO has authority to approve/disapprove extensions on the recommendation of the NOC Controller or SCO/Watch Officer of up to 1 hour to complete ongoing scheduled ASIs within CONUS. The GNSC SCO will notify the GNC SCO that an extension was granted. Extensions beyond 1 hour require DISA CONUS Commander approval and will be coordinated with the GNC SCO after mission impact has been jointly assessed by the GNSC and GNC SCO.

If an ASI has to be cancelled, the Node Site Coordinator or NOC Controller or SCO/Watch Officer will notify the DISA CONUS ASI Manager immediately or the GNSC SCO (after hours). The ASI Manager will notify the users by sending a cancellation message and the reason for cancellation to the field. If the cancellation comes immediately prior to the maintenance, then telephonic notification between the applicable NOC and users is authorized. An official cancellation/reschedule message will be sent as soon as possible.

#### **2.6.8 CARRIER RATES (T1, E1, OC3, OC12, ETC)**

A carrier signal is a frequency in a communications channel modulated to carry analog or digital signal information. For example, an FM radio transmitter modulates the frequency of a carrier signal and the receiver processes the carrier signal to extract the analog information. An AM radio transmitter modulates the amplitude of a carrier signal.

- T1: A dedicated connection supporting data rates of 1.544Mbps. A T-1 line actually consists of 24 individual channels, each of which supports 64Kbps. Each 64Kbps channel can be configured to carry voice or data traffic. T-1 lines are a popular option because they allow for Internet connectivity. The Internet backbone itself consists of faster T-3 connections.

- E1: Ten years following the success of the T1, Europe decided they wanted their own digital transmission technology and subsequently developed the E1. An E1 connection supports 2.048Mbps. The E1 and T1 can be interconnected for international use. Europe has E carrier ratings from E1 to E5 with E5 supporting 565.148Mbps.

- T3: A dedicated connection supporting data rates of about 43Mbps. A T-3 line actually consists of 672 individual channels, each of which supports 64Kbps. T-3 lines are used mainly by Internet Service Providers (ISP) connecting to the Internet backbone and for the backbone itself.

- OC: Is short for Optical Carrier, used to specify the speed of fiber optic networks conforming to the SONET standard. Below are the speeds for common OC levels:

OC = speed

OC-1 = 51.85 Mbps  
OC-3 = 155.52 Mbps  
OC-12 = 622.08 Mbps  
OC-24 = 1.244 Gbps  
OC-48 = 2.488 Gbps  
OC-192 = 9.952 Gbps  
OC-255 = 13.21 Gbps

### **2.6.9 IT-21**

IT-21 is an information transfer strategy that provides Network Connectivity capable of Voice, Data and Video for afloat units. It provides access to NIPRNET, SIPRNET and JWICS, and supports all tactical and non-tactical mission areas. IT-21 uses Commercial Off the Shelf (COTS) Technology to keep ships updated with the most modern equipment. The goal of IT-21 is to provide an integrated, coordinated, end-to-end warfighting capability.

#### **2.6.9.1 INTEGRATED SHIPBOARD NETWORKING SYSTEM (ISNS)**

ISNS is a collection of workstations, servers, switches and routers, both at the Unclas and Secret levels that connect numerous systems like GCCS-M, NTCSS, SAMS, OPINS etc., to external routers like ADNS. It provides Navy ships with reliable, high-speed SECRET and UNCLASSIFIED Local Area Network (LAN)s; Network infrastructure (switches routers, and drops to the PC); Basic Network Information Distribution Services (BNIDS); Access to the DISN Wide Area Network (WAN); Secure and Non-secure Internet Protocol Router Network -SIPRNET and NIPRNET, used by other hosted applications (i.e. NTCSS, GCCS-M, DMS, NSIPS, NAVMPS, TBMCS, and TTWCS) and enables real-time information exchange within the ship and between afloat units, Component Commanders, and Fleet Commanders. Figure 2-6 depicts a generic ISNS architecture.

# Generic ISNS Architecture (ATM/GigE/Fast Ethernet)

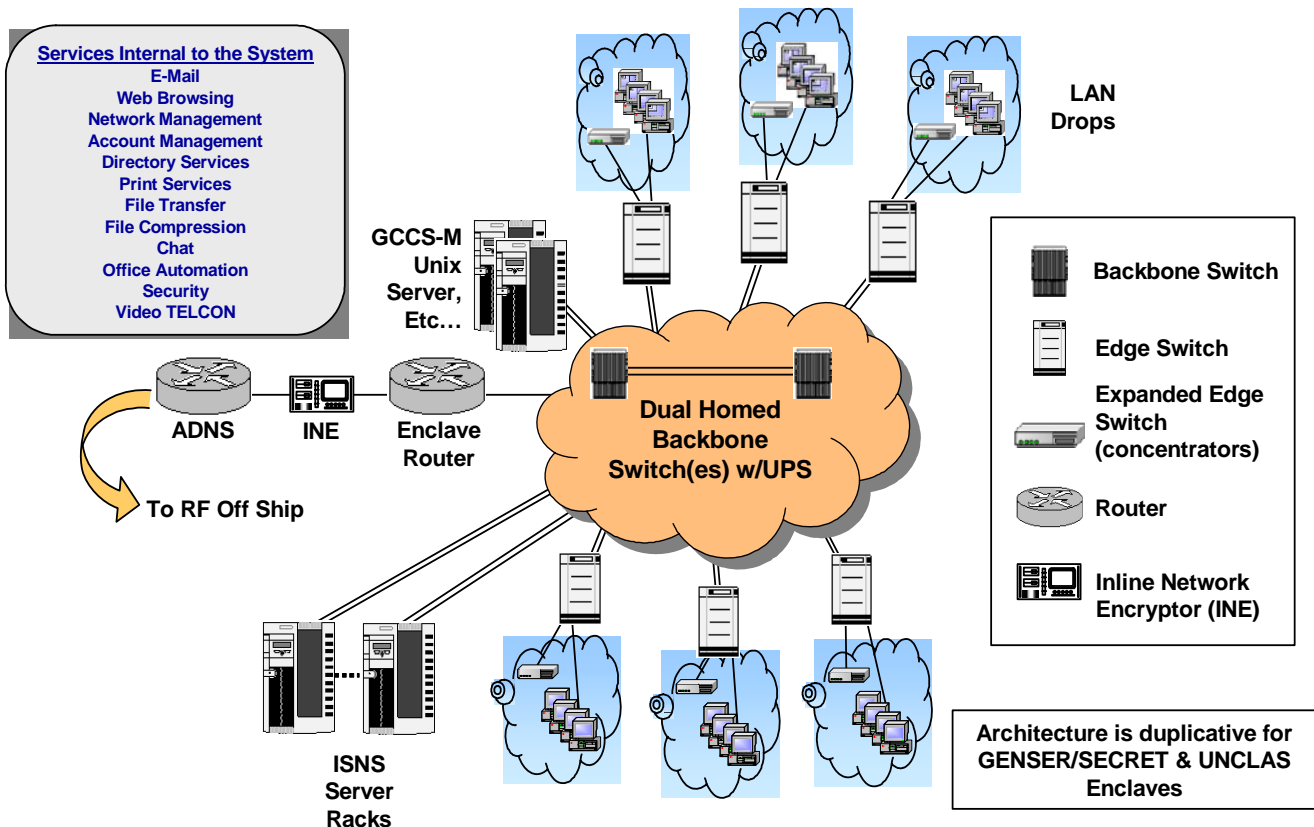


Figure 2-6  
ISNS Architecture

## 2.6.9.2 NAVAL TACTICAL COMMAND SUPPORT SYSTEM (NTCSS)

NTCSS' goal is to provide tactical automated support for maintenance, supply, financial, material and personnel administrative matters. Using IT-21, the Navy-Marine Corps Intranet (NMCI) communication links, and COTS software, NTCSS hopes to achieve bi-directional database replications. Replicating administrative information will reduce the warfighter's workload.

## 2.6.9.3 FLEET NETWORK OPERATIONS CENTERS (FLTNOC)

Naval shore communications has evolved from a series of isolated shore based radio stations to a highly sophisticated communications infrastructure. The requirement to support



integrated voice, video, and data has increased the complexity of a typical communications shore station. Consequently, The Naval Computer and Telecommunications Area Master Stations (NCTAMS) were developed to provide operational direction and management oversight to all subordinate telecommunications system users.

The IT-21 FLTNOCs provide a number of critical Internet Protocol (IP) services to the Fleet (both deployed and pier side) and act as regional gateways to the Defense Information Systems Network (DISN) IP networks in each of their respective Areas of Responsibility (AOR). This is accomplished through the use of a flexible network architecture that can meet unique needs of the different regional forces. The FLTNOCs were originally established as independent data communication systems that only serviced units within specific coverage areas.

The nomenclature for FLTNOCs is AN/FSQ-206. The Navy currently has four sites designated as IT-21 FLTNOCs': European Central Region Network Operations Center (ECRNOC) NCTS Naples Italy, Indian Ocean Region Network Operations Center (IORNOC) NCTS Bahrain, Pacific Region Network Operations Center (PRNOC) NCTAMS PAC and Unified Atlantic Region (UARNOC) NCTAMS LANT. The four IT-21 FLTNOCs are geographically dispersed around the world to service deployed users, provide the entry points for Navy Tactical Satellite Systems and also operate and maintain one or more Defense Satellite Communications Systems (DSCS) terminals. Each IT-21 FLTNOC is typically responsible for providing services to Fleet users located in their corresponding AOR. Current technology provides the ability for a unit to be terminated via satellite RF and terrestrial paths at almost any FLTNOC, regardless of geographical location. FLTNOCs are designed to provide IP services to Fleet IT-21/Integrated Shipboard Network System (ISNS) and deployed ground forces. All are capable of flexibly providing IP services based on unit's satellite RF capabilities including multiple simultaneous RF paths using Automated Digital Network System (ADNS), Automated Digital Multiplexing System (ADMS) or legacy.

The current IT-21 FLTNOC network architecture operates as individual ingress and egress points for Forward Deployed Naval Forces (FDNF) within their specific AOR to provide connectivity to the DISN. Connectivity to the IT-21 FLTNOC from the FDNF afloat platforms is primarily done via the ADNS, which uses available satellite communications systems to enable ship-to-shore data connectivity. Exceptions to this configuration exist, dependant upon the individual mission of the FDNF unit or IT-21 FLTNOC, and are handled on a case-by-case basis. Each IT-21 FLTNOC provides local back-up and restore services via the Network Attached Storage (NAS) and the Out of Band Network, but does not provide for off-site backup and restore services. Figure 2-7 provides a list of baseline equipment for the IT-21 FLTNOC per enclave.

NOC Equipment	Description/Use
Premise Router	Connection point for each NOC to the DISN network.
Outer Security Screening Router (OSSR)	Security filtering for outside the firewalls. Provides load balancing for the Bastion Hosts via VLAN with ISSR.
Firewalls	Bastion hosts. Provides packet filtering, application and layer 4-proxy services.
Inner Security Screening router (ISSR)	Security filtering inside the firewalls. Provides load balancing for the Bastion Hosts via VLAN with OSSR.
Service Switch	Load balances internal DNS, Email, virus scan and web services.
Virus Scanners	Scans inbound and outbound Email and attachments for viruses.
DNSMail Servers	DNS and Email (SMTP) store and forwarding services.
Fleet Router	Serial and IP connectivity to the ADNS network and IT-21 FLTNOC RF (legacy serial) connectivity.
Tunnel Router	Generic Routing Encapsulation (GRE) tunneling services to the Fleet in order to establish NIPRNet Open Shortest Path First (OSPF) adjacencies across the ADNS network.
Network Encryption System (NES) Inline Network Encryptor (INE) Tactical Local Area Network Encryptor (TACLANE)	Encryption devices.
Dial-in switch	Provides in-line connectivity to the Fleet Router
POTS and Integrated Services Digital Network (ISDN) dial-in Routers	Provides dial-in services over telephone or ISDN lines.
Management Switch	Provides connectivity for management devices

**Figure 2-7**  
**NOC Core Equipment**

Figure 2-8 depicts a simplified topology of the current IT-21 FLTNOG architecture and displays only the core equipment for a single enclave (from the Premise Router to the Fleet Router). For the sake of brevity, server subsystems are indicated as Service Suites and do not display the correct number of servers. For example, each IT-21 FLTNOG has at least five DNS Mail servers but is displayed as a single Mail/DNS Suite. Other suites that make up the IT-21 FLTNOG are the Firewall, Virtual Private Network (VPN), Intrusion Detection, Virus Scan, and Web Cache suites. The Premise Router is the ingress and egress Point of Presence (POP) for the IT-21 FLTNOG to the DISN and is considered an untrusted interface. The Fleet Router is the ingress and degree POP to the ADNS network, and is considered a trusted network. This trusted network is the user side of the network system. Also note the External DNS Suite in the below diagram. Fleet NOCs use a feature called Split Horizon DNS. This is used to provide different DNS query answers to requests initiated outside the enclave. If the DNS zone is active internally (inside a FLTNOG enclave), the DNS/Mail Suite provides the actual answers to a DNS query that can associate an IP address to a ship if the query is initiated from inside the enclave. To minimize configuration changes when ships traverse from one AIR to another, the IT-21 FLTNOGs utilize secondary IP addresses called Virtual IPs (VIP), which are duplicated between each IT-21 FLTNOG. Using VIP addresses helps to simplify configuration management and obviates configuration changes to the ship networks or servers for INCHOP/OUTCHOP. VIPs are used for DNS forwarding, Simple Mail transfer Protocol (SMTP) relay and Network Time Protocol (NTP).

All unclassified voice and IP data traversing the classified enclave for ship and shore commands is encrypted using a NES 4001A, INE KG-235 or a TAFLANE KG-175.

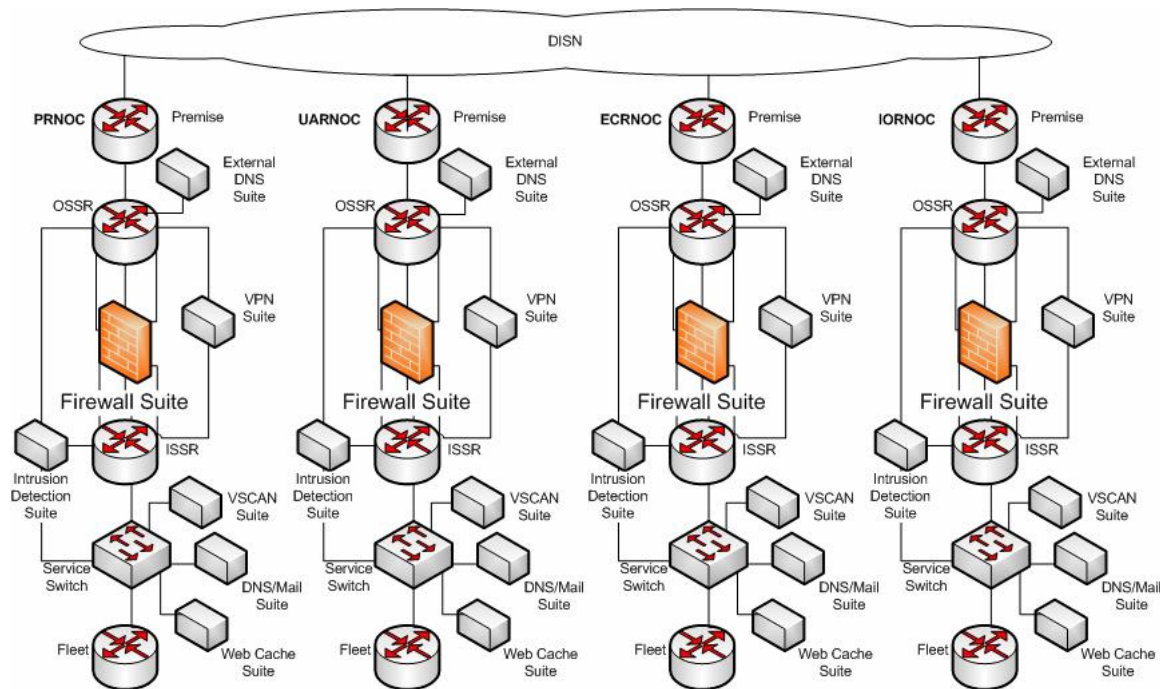


Figure 2-8

## IT-21 FLTNOG Architecture

## 2.6.9.3.1 INCHOP/OUTCHOP

To obtain IP services from a FLTNOG the following criterion must be met:

1. Must have a valid Interim Authority to Operate (IATO) or Authority to Operate (ATO) obtained from NETWARCOM Designated Approving Authority (DAA). The unit Information Assurance Manager (IAM) can provide guidance on validating or obtaining an (I)ATO.
2. Submit an IP services request message in accordance with Global Communications Information Bulletin (GCIB) 3A.
3. If service will be provided via satellite communications link, a valid Satellite Access Authorization (SAA) for the intended satellite RF path is required.

The current system allows Fleet units to transit between AORs without making configuration changes to their ISNS equipment. This is facilitated by default configurations in the ADNS and the ISNS that utilize the IT-21 FLTNOG's VIP address scheme. With the exception of physical path connectivity, the gaining FLTNOG drives the Change of Operational Control (CHOP) process. Once the satellite communications link has been terminated at the gaining Technical Control Facility (TCF, the IT-21 FLTNOG will enable the Fleet unit(s) DNS zone on the internal DNSMail servers. All zone

changes through the entire INCHOP/OUTCHOP process are accomplished by using either the NOC management web interface of the DNSMail servers command line. The Fleet unit(s) IP addresses are then added to the "trusted networks" table on the Navy Firewall Security System (NFSS). The Fleet unit(s) homeport IT-21 FLTNO, which is authoritative for their DNS zone resolution, will be notified by the gaining IT-21 FLTNO to direct the Fleet unit(s) external Mail Exchanger (MX) record to the gaining IT-21 FLTNO. After the gaining IT-21 FLTNO has verified IP connectivity for the fleet unit(s), their losing IT-21 FLTNO is notified to deactivate the Fleet unit's DNS zone(s) on their DNSMail servers. Service verification is accomplished by a test email from the IT-21 FLTNOs domain to the Fleet unit(s) domain (i.e., a successful email transfer between ior.navy.mil and Washington.navy.mil). The only exceptions are for embarked units that must have a CHOP in and out of the Navy IT-21 FLTNOs (e.g. Marine Expeditionary Units (MEUs) that move from Navy and Marine NOCs)). Additionally, the gaining IT-21 FLTNO is also responsible for ensuring the unit's IP address Classes Inter-Domain Routing (CIDR) block is being advertised via the IT-21 FLTNO connection to DISN.

#### **2.6.9.3.2 IT21 FLTNO SECURITY**

The security posture for each IT-21 FLTNO is independently administered but centrally governed by the Chief of Naval Operations (CNO)/NETWARCOM Unclassified Trusted Network Protect (UTN Protect) firewall policy. Use and enforcement of this policy is mandated by CNO and NETWARCOM security policies. IT-21 FLTNOs are also tasked with implementing IP block lists and DNS black hole lists as promulgated by Navy Cyber Defense Operations Center (NCDOC).

#### **2.6.9.3.3 CUSTOMERS AND SUPPORT**

The following section details the personnel who are currently involved in the day-to-day operations of an IT-21 FLTNO. There are several types of customers in the IT-21 FLTNO environment. The customers utilizing satellite or pier connectivity for IT-21 FLTNO access represent the Fleet users. Additionally, there are embarked units such as air wings and command staff who also utilize the ship and IT-21 FLTNOs assets for services. It is also important to note that the NCTAMS and/or NCTS may be serving local customers that do not fall within the IT-21 FLTNO Program, but require service.

The IT-21 FLTNOs utilize a multi-layered support concept. Each support tier is discussed in further detail below:

1. Tier One - Provided 24/7 by the active duty Watch section. This support includes troubleshooting ship-to-shore and intra-NOC communications and acts as the primary resource for IT-21 FLTNO operations. Daily

configuration changes and maintenance of the system are also performed.

2. Tier Two - System Administrators are responsible for the providing the highest state of operational readiness and availability of the IT-21 FLTNOC to the Fleet.
3. Tier Three - Provided by the Fleet Systems Engineering Team (FSET) engineers which provide specialized system technical support, engineering assistance, and on site training for all NCTAMS/NCTS personnel.
4. Tier Four - SPAWARSYSCEN Charleston acts as the primary engineering activity for IT-21 FLTNOC development and provides In-Service Engineering Activity (ISEA) support for the FSETs, NCTAMS, NCTS and other Fleet services. The ISEA also provides logistics for equipment replacement, testing, and training, and as well as hardware and software upgrades for all IT-21 FLTNOCs. The ISEA contacts and interfaces with commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) vendors as necessary for technical support.

#### **2.6.9.3.4 NAVY REGIONAL NETWORK OPERATIONS AND SECURITY CENTER (NAVRNOSC)**

The ultimate goal is to migrate from the current four Fleet NOCs concept into expanded roles within NAVRNOSCs. ECRNOC and IORNOC will eventually be collapsed and UARNOC and PRNOC will remain essential elements within RNOSC East and RNOSC West respectively. While they will continue to support the service provider functions of the NCTAMS in addition to managing their portion of the Navy Enterprise Network (NEN), they will also provide virtual views of the enterprise at the strategic, operational and tactical levels. The NAVRNOSCs serve as the technical arm for the Navy in aggregating the elements of Network Operations (NetOps) including Enterprise Management (EM), Network Defense (ND), and Content Management (CM), which supplements Situational Awareness (SA) and Command and Control (C2), employed to operate and defend their portions of the NEN. The NAVRNOSC provides network and system status, performance and ND events from outlying CONUS and OCONUS elements including the OCONUS Navy Enterprise Network (ONE-NET), IT-21, Network Operations Centers and other systems.

The NAVRNOSC will monitor and control faults, configuration accounting, performance and security of the NEN elements for which they have operational responsibility. The NAVRNOSC will coordinate closely with, and provide users and higher echelons with network status reports and access to real-time data. Additionally, the NAVRNOSC will maintain records pertaining to customer information, local tier control center and site coordinator contact information, network resources, faults and

outages. NAVRNOSC operators will have the capability to remotely manage and control lower echelon systems through the Enterprise Network Management System (ENMS). ENMS has a suite of EM, ND, CM, C2 and SA tools that can be leveraged to provide a common NAVRNOSC operational picture to the Navy Global Network Operations and Security Center (NAVGNOSC).

**2.6.9.3.5 PROGRAM EXECUTIVE OFFICE, COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS AND INTELLIGENCE (PEO C4I) INTELLIGENCE (PEO C4I)**

PEO C4I is the program manager for the NOC system and as such is responsible for its life cycle management. As the acquisition agent, PEO C4I is accountable for cost, schedule, and performance. Two program offices within PEO C4I have responsibility for different subsystems. PMW 160 has program management responsibility for the Information Assurance (IA) product suite and PMW 790 has responsibility for the rest of the equipment. Once deployed and fielded, the architecture is supported and maintained with NCTAMS/NCTS personnel. SPAWARSYSCEN Charleston provides technical oversight and engineering support as directed by the PMWs.

**2.6.10 NAVY MARINE CORPS INTRANET (NMCI)**

The Navy/Marine Corps Intranet (NMCI) was developed to procure and manage information technologies (IT) for the Navy at the enterprise level. NMCI is a partnership between the Navy and industry whereby industry provides IT services purchased by individual Navy commands. The key point is that the Navy does not own or manage the hardware, software, or communications infrastructure. Rather, a command purchases the IT services it requires from a catalog of standard services, and industry will then provide the necessary hardware and infrastructure to deliver those services. Performance requirements for each service are governed by standard Service-Level Agreements (SLAs) to ensure that the command's operational requirements are met.

The NMCI contract was designed to support all basic networking needs of shore users to include:

Network access:

1. NIPRNET
2. SIPRNET
3. Fleet NOC/USN ships
4. Internet (via NIPRNET)
5. Ships via piers
6. Legacy USN networks (Non-NMCI standard).

End-user services:

1. Standard office suites

2. Web hosting and browsing
3. E-mail.

Key concepts that contribute to the full operational capabilities of NMCI include:

1. Standardizing DON (Navy and Marine Corps) policies, architectures, and products.
2. Providing basic protection across the DON via the Regional Network Operations Centers (RNOCs) to include piers, bases, commands, posts, and stations.
3. Maximizing use of commercial off-the-shelf (COTS) internet technology security components (i.e., firewalls, intrusion detection, virtual private network (VPN), virus scanning, etc.).
4. Hardening infrastructure and diverse connections (i.e., protect against denial of service and/or respond to existing vulnerabilities).

NMCI physical infrastructure consists of numerous LANs connected by base area networks (BANs) for each base or region. Base and regional server and data farms with associated support staffs provide data services. The BANs are connected by two separate WANs to form the Navy enterprise network. Network management and monitoring is provided by four NOCs located at Norfolk, VA; San Diego, CA; Pearl Harbor, HI, and Quantico, VA.

NMCI is designed to provide end-to-end communications within the Navy, seamlessly integrating with afloat naval forces.

#### **2.6.11 OVERSEAS NAVY ENTERPRISE NETWORK (ONENET)**

Commands in each region operate and maintain their own IT infrastructure. The Navy is presently extending its enterprise network OCONUS under the ONE-Net modernization program at 16 major fleet concentration areas:

1. Europe – Naples, London, Rota, Souda Bay, Sigonella, and La Maddalena.
2. Pacific Far East – Yokosuka, Sasebo, Misawa, Atsugi, Okinawa, Korea, Guam, Singapore, and Diego Garcia.
3. Middle East – Bahrain.

ONE-Net is intended to replace legacy Navy IT networks and will serve an OCONUS population of 26,000 users. ONE-Net will implement a gigabit Ethernet backbone network on Navy and Marine Corps bases located OCONUS. The ONE-Net architecture is modeled



after the NMCI design in order to insure compatibility and connects to NMCI and afloat networks via the DISN.

In addition to shore networks, ONE-Net has installed network connectivity at CONUS and OCONUS piers at Pearl Harbor, Japan, and Guam. There are validated additional requirements for OCONUS pier side connectivity at Italy, Spain, and Greece.

Operation of ONE-Nets is envisioned to be taken over by NMCI; however, host-nation agreement (HNA) and status-of-forces agreement (SOFA) issues need to be resolved beforehand. Therefore, the Navy Network OCONUS will continue to operate as a Government-Owned/Government-Operated (GOGO) network until transition to a Contractor-Owned/Contractor-Operated (COCO) environment occurs under NMCI.

#### **2.6.12 CONSOLIDATED AFLOAT NETWORKS AND ENTERPRISE SERVICES (CANES)**

##### **BACKGROUND:**

Over the last two decades, the explosion of networking capability has created unintended consequences aboard afloat platforms. For each type of network requirement the navy identified (e.g., tactical, administrative, classified, coalition, etc.), a separate, distinct network was developed and installed. As a result, the navy's program office for Networks, Information Assurance and Enterprise Services manages a portfolio of multiple, unique networks with various classification levels, operating systems, and protocols. These individual networks are difficult to certify and defend from attacks; they bring their own racks and servers; and they are unable to share server and storage resources. As a result, the space, weight and power required have reached capacity on many platforms.

In order to address these challenges, the program office developed a phased plan to migrate its primary network programs into a single overarching program called Consolidated Afloat Networks and Enterprise Services (CANES). CANES will have at its roots primarily the Integrated Shipboard Network System (ISNS), but will also incorporate the capabilities of other networks such as Combined Enterprise Regional Information Exchange System (CENTRIXS); the Sensitive Compartmented Intelligence Local Area Network (SCI-LAN); and the Submarine LAN.

The basic concept of CANES is to take hardware requirements and create a single consolidated computing environment using standard network infrastructure and a common rack architecture. Enterprise services will support hosting of both warfighting and administrative application programs. This evolution requires detailed technical exchanges between the programs' engineers and a significant amount of resource reprogramming.

CANES is a CNO-directed approach to reduce infrastructure and

provide increased capability across the afloat enclaves. It provides technical and programmatic realignment of afloat infrastructure and services, utilizing Open Architectures. CANES will replace ISNS.

CAPABILITIES:

1. Voice Services
  - a. IP Telephony
  - b. Mobile and Stationary
  - c. Secure and Un-Secure
2. Video Services
  - a. Video Teleconferencing
  - b. Video/Graphics Distribution
3. Data Services
  - a. Network Support
  - b. Information Management
  - c. Core Infrastructure Services
  - d. Network Access (IPv4/IPv6 Capable)
  - e. Information Delivery
4. Systems Management
  - a. Performance, Availability, & Service Level Mgmt
  - b. Fault, Problem, Incident, & Service Desk Mgmt
  - c. Configuration, Change, & Release Mgmt
  - d. Security Mgmt, IA, CND
  - e. Capacity Mgmt

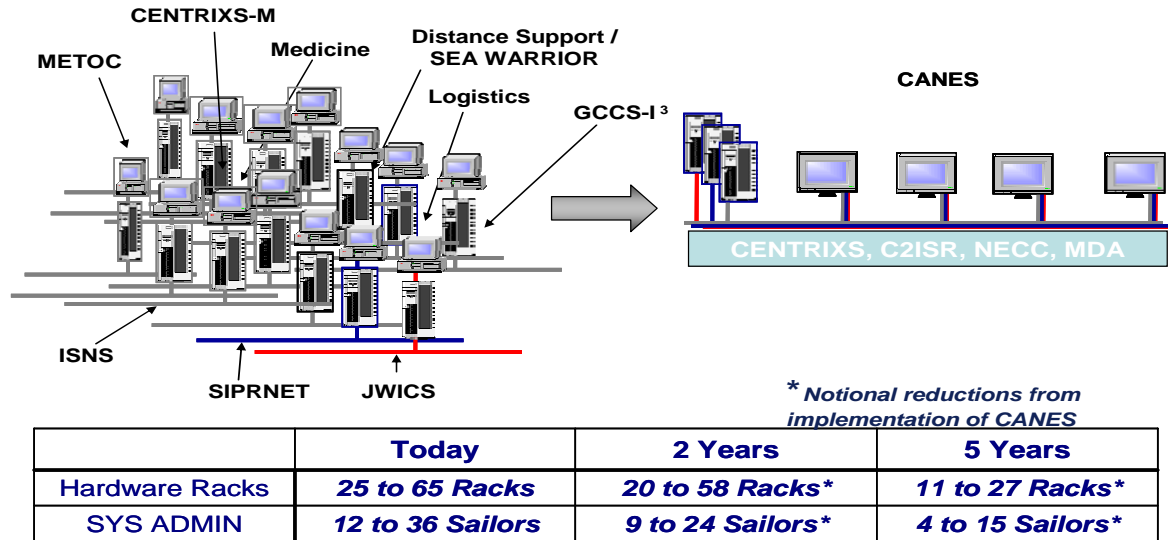


Figure 2-9  
CANES CCE infrastructure

2.6.13 GLOBAL INFORMATION GRID - BANDWIDTH EXPANSION (GIG-BE)

The Global Information Grid (GIG) bandwidth Expansion (GIG-BE) is key to realizing the Department's enterprise information environment. It is providing a worldwide, ground-based fiber-optic network that will expand Internet-Protocol (IP)-based connectivity and at the same time effectively and efficiently accommodate older, legacy command, control and communications (C3) systems. This enables an exponential leap in ground-based voice, video and data exchange capabilities for the Department of Defense and the intelligence community.

GIG-BE created a ubiquitous "bandwidth-available" environment to improve national security intelligence, surveillance and reconnaissance, and command and control information sharing. To implement GIG-BE, DISA is aggressively enhancing the existing end-to-end information transport system, the Defense Information System Network (DISN), by significantly expanding bandwidth and physical diversity to selected locations worldwide. The program provides increased bandwidth and diverse physical access to approximately 100 critical sites in the continental United States (CONUS) and in the Pacific and European theaters. These locations are interconnected via an expanded GIG core. Specifically, GIG-BE connects key intelligence, command and operational locations with high bandwidth capability over physically diverse routes, and the vast majority of these locations will be connected by a state-of-the-art optical mesh network design.

#### 2.6.14 HIGH SPEED GLOBAL RING (HSRG)

The AN/USQ-169B(V)1 High Speed Global Ring (HSGR) provides increased capacity and connectivity in the transport communications links between major Naval ashore claimants. The HSGR transforms the legacy AN/USQ-169A(V)1 Automated Digital Multiplexing System (ADMS) shore connectivity architecture into an integrated network of transport services that provides the warfighter with a dynamic, reliable, flexible and restorable transport service capability. The HSGR enables implementation of new and improved capabilities. These include Fleet Network Operation Center (FLTNOG)-to-FLTNOG connectivity and Joint Service Imagery Processing System-Navy Concentrator Architecture (JCA) connectivity.

The primary purpose of the HSGR is to provide an increased transport link between NCTAMS PAC, NCTS San Diego, NCTAMS LANT, NCTS Naples, Italy and NCTS Bahrain. The HSGR network utilizes ATM, which provides transport services for high speed classified and unclassified IP networks as well as existing Legacy to major shore sites. All IT-21 IP traffic bound for another IT-21 resource will remain on Navy controlled networks utilizing the HSGR. The HSGR uses Marconi TNX-1100 and Lucent PSAX 2300 Asynchronous Transfer Mode (ATM) switches interconnected via DISN ATM services or commercial leased lines to interconnect the two NCTAMS, NCTS San Diego, NCTS Naples, Italy and NCTS Bahrain. The HSGR is depicted in Figure 2-10 and 2-11.

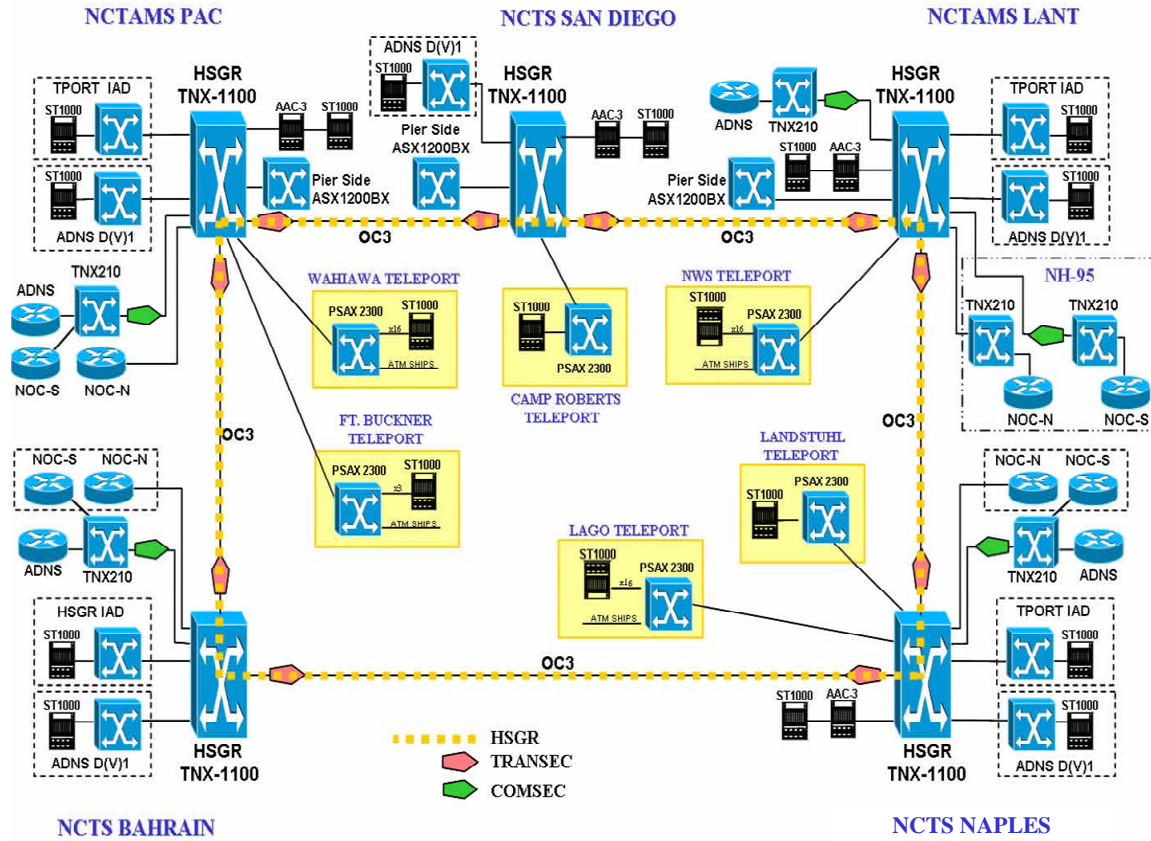
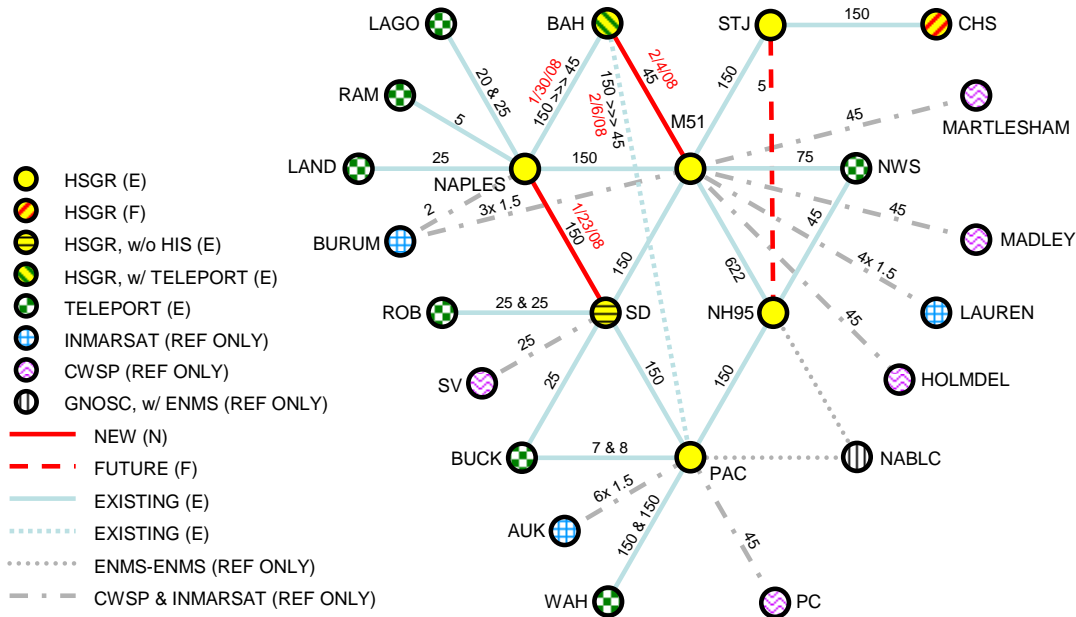


Figure 2-10  
High Speed Global Ring Architecture



**Figure 2-11**  
**High Speed Global Ring mesh topology**

**2.6.14.1 HSGR ADVANTAGES**

An ATM backbone enables reconfigurable class and Quality of Service (QoS) parameters for data transport supporting tactical users. ATM is a dedicated connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. Individually, a cell is processed asynchronously relative to other related cells and is queued before being multiplexed over the transmission path. ATM transmission rates operate at either OC-3 (155 Mbps) or OC-12 (655 Mbps), though speeds on ATM networks can reach up to OC-192 (10 Gbps). Operationally, the HSGR architecture supports the following critical warfighting requirements:

1. Increased bandwidth capacity between major shore facilities to support the requirements of the warfighter, to include:
  - a. Near-real-time access to information and network services.
  - b. Support shipboard terminations above 2 Mbps.

2. Automated Digital Network System (ADNS) Increment (INC) II/III load distribution, to include:
  - a. Provide primary path for Unclassified (UNCLAS) traffic with Commercial Wideband Satellite Program (CWSP) capable ships terminated in NCTS Naples, Italy or NCTS Bahrain.
  - b. Provide failover path for all classes of traffic over CWSP when Defense Satellite Communications System (DSCS) is unavailable.
  - c. Provide failover path for JCA traffic when CWSP path is unavailable.
3. Provide for FLTNOG-to-FLTNOG (N2N) and other inter-theater network services restoral.
4. Super High Frequency (SHF) connectivity restoral.
5. Consolidation of other program of record terrestrial leases, to include transition of existing ADMS trunks across the HSGR backbone.
6. Interface with Department of Defense (DoD) Transformational programs (e.g. DoD Telecommunications Portal (TELEPORT), Global Information Grid (GIG)-Bandwidth Expansion (BE) and Transformational Communications Architecture [TCA]).

The ADNS to HSGR interface bandwidth is currently rated at OC-3 (155 Mbps) with future growth to OC-12 (655 Mbps). However, the current provision for ADNS traffic across the ring is 18 Mbps. The HSGR as the Navy shore ground transport architecture creates an infrastructure to provide new Fleet services, improve performance and reliability for Fleet services and creates a flexible infrastructure that scales for the consolidation or expansion of FLTNOG services. Additionally, it also provides the infrastructure to deploy enterprise collaboration tools and applications that were previously blocked by the Fleet boundary firewalls.

#### **2.6.14.2 HSGR NETWORK MANAGEMENT**

Network Management refers to the broad subject of managing computer networks, using a variety of tools, applications and devices. HSGR Network Management is accomplished through:

1. Direct connect (console)
2. Remote (IP, SNMP)
3. Distributed Local Area Network (LAN) Emulation (DLE)

The following tools are used in support of network management of the HSGR:

1. Service On Data (SOD) is a Marconi product that was implemented to provide management capabilities for the HSGR core ATM switches.
2. Lucent AQueView is a Simple Network Management Protocol (SNMP) based software suite that provides management capabilities for the Lucent PSAX edge ATM switches.
3. Solarwinds software package to analyze bandwidth throughput.

#### 2.6.15 N2N - NOC TO NOC

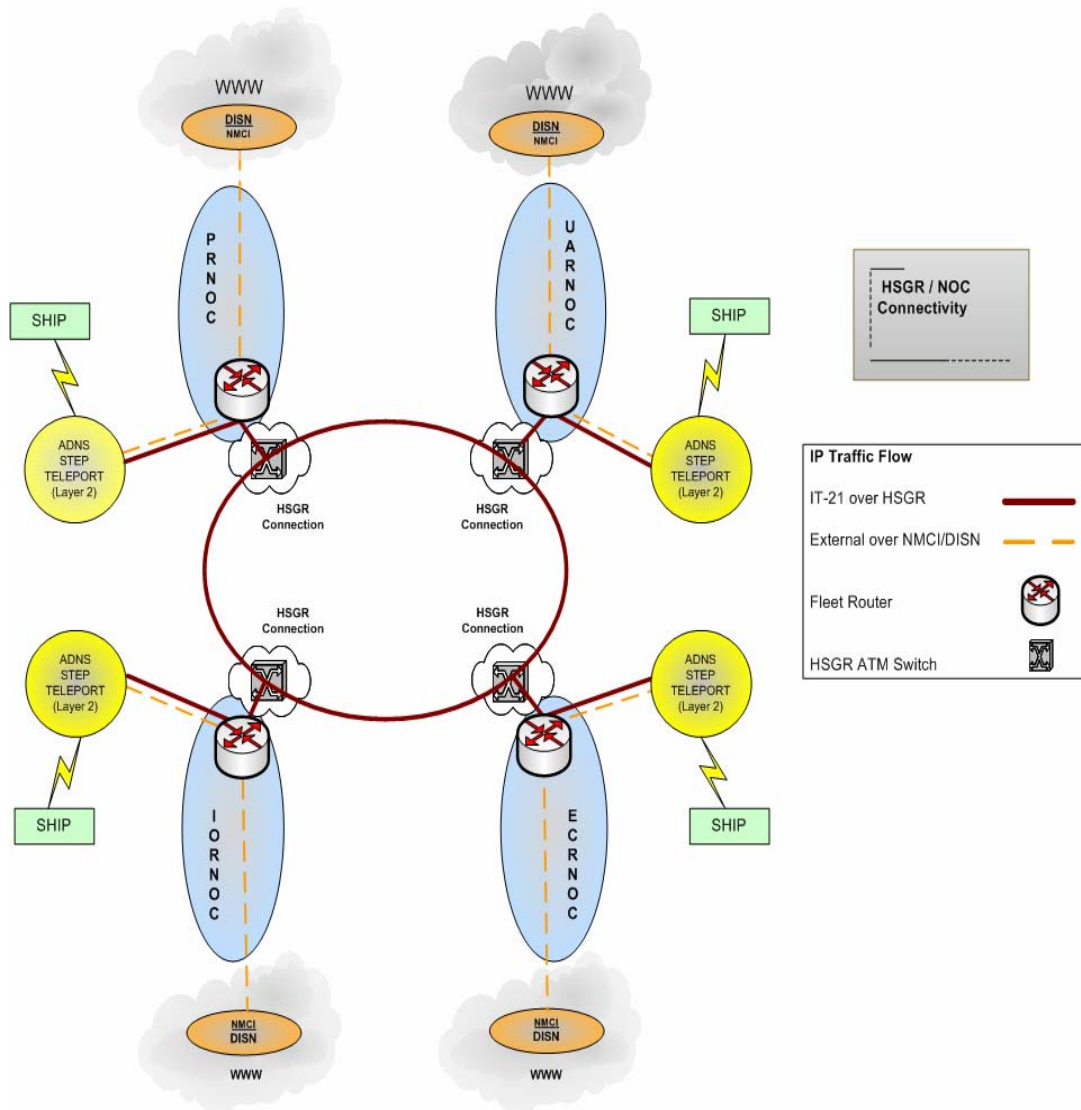
There are four IT-21 FLTNOCs geographically dispersed around the world to service deployed users. Each IT-21 FLTNOC is typically responsible for providing services to Fleet users located in their corresponding AOR. The four independent FLTNOCs have their own separate connectivity centers and do not exchange data directly with other FLTNOCs. The IT-21 FLTNOCs are located at the following locations:

1. **European Central Region** (ECRNOC)- NCTS Naples, Naples, Italy
2. **Indian Ocean Region** (IORNOC)- NCTS Bahrain, Manama, Bahrain
3. **Pacific Region** (PRNOC)- NCTAMS PAC, Wahiawa, Hawaii
4. **Unified Atlantic Region** (UARNOC)- NCTAMS LANT, Norfolk, Virginia

As the Navy migrates towards a two Regional Network Operations and Security Center (RNOSC) and one Global Network Operations and Security Center (GNOSC), the evolution of IP services will become more simplified. The IT-21 FLTNOCs provide a number of critical Internet Protocol (IP) services to the deployed Fleet in each of their respective Areas of Responsibility (AORs). This is accomplished through the use of a flexible network architecture that can meet unique needs of the different regional forces. These FLTNOCs were originally established as independent data communications systems that only serviced units within specific coverage areas.

N2N leverages the connectivity and capabilities of the High Speed Global Ring as a transport. Access points to the HSGR terminate within each FLTNOC, allowing the ability to route Internet Protocol (IP) data to each other without having to traverse through Defense Information Systems Network (DISN), and subsequently, the destination FLTNOCs Boundary 1 (DISN facing) firewall architecture. Figure 2-12 provides an overview of the HSGR and its entry points into each FLTNOC:





**Figure 2-12**  
**High Speed Global Ring to FLTNOC entry points**

The upshot of implementing N2N is FLTNOC interconnectivity and restoral capability should a FLTNOC lose connectivity on their DISN path. If a FLTNOC is unable to utilize their DISN connection, their outbound network traffic will automatically be diverted across the HSGR to another FLTNOC to utilize their DISN path.

The establishment of N2N allows the following capabilities that were previously unavailable:

1. Transform four independently operated FLTNOCs into a single unified IT-21 FLTNOC Enterprise, providing transparent redundant services and security to the Fleet.

2. Provides the infrastructure to deploy Enterprise collaboration tools and applications that were previously blocked by the Fleet Boundary 1 firewall.
3. Enhanced security by keeping Fleet traffic on Navy controlled networks.
4. Enhanced security by providing an Enterprise wide view of security management and monitoring devices.
5. Improved ability to withstand denial-of-service attacks.
6. Enhanced network monitoring by providing an Enterprise view of all IT-21 FLTNOG circuits, servers, and equipment.
7. Improve configuration management by providing the infrastructure for a central repository for system configurations (server/router/switch configurations).
8. Eventually, with the exception of embarked units (e.g. CVW or CCSG), the need for IT-21 FLTNOG system configuration changes when ships move between AORs will be eliminated.
9. Provide continuity of service for the Fleet in the event of IT-21 FLTNOG outages.

#### **2.6.15.1 N2N REMOTE RESTORATION**

The N2N Enterprise Network provides the framework for connectivity to a central repository, which maintains configuration management and off-site backups of FLTNOG assets. A FLTNOG can retrieve device configurations from the central repository if necessary.

#### **2.6.15.2 N2N SECURITY**

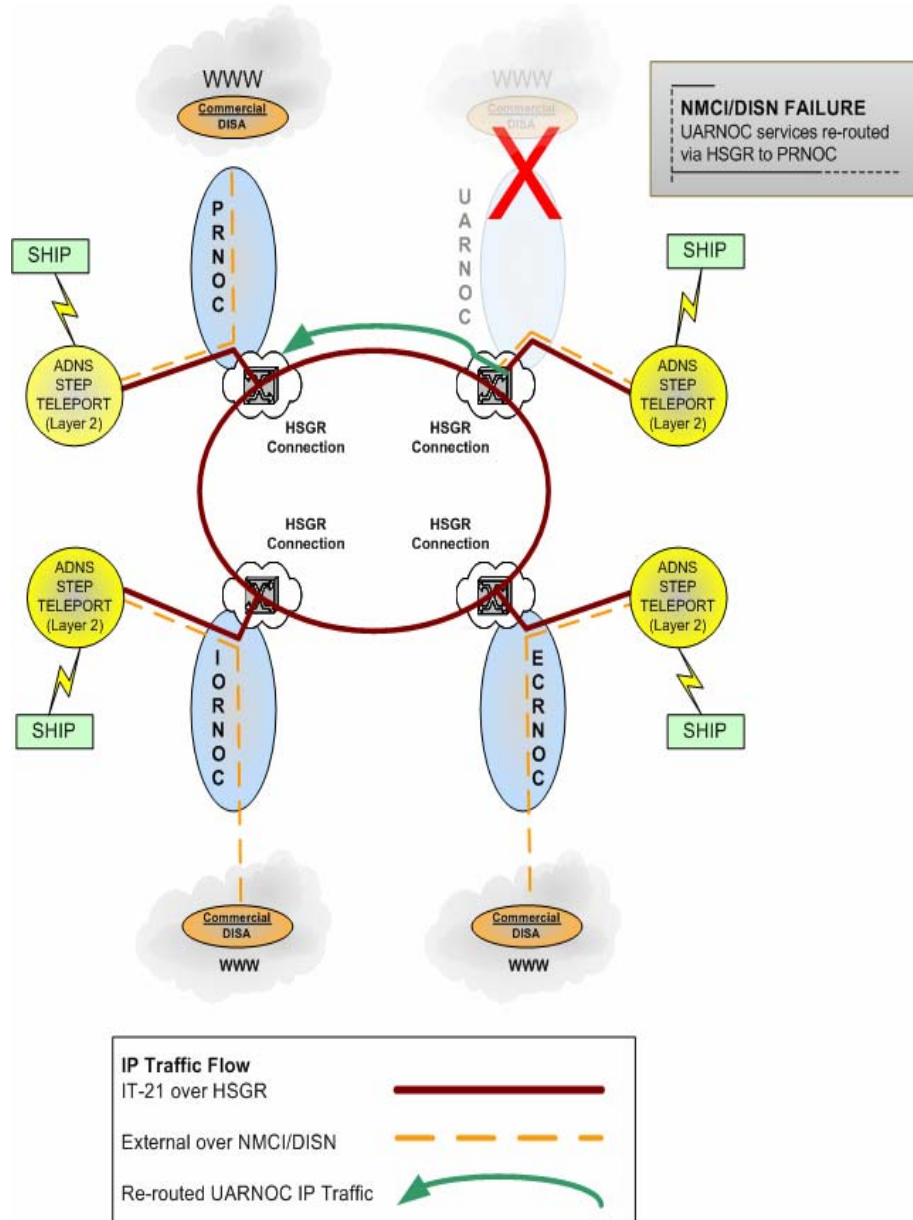
Security in the N2N Enterprise Network architecture is addressed on multiple levels to include global policies, procedures and configuration management, and, inter and intra-IT-21 FLTNOG network device security. The routing architecture will be authenticated and encrypted where applicable which reduces the possibility of a false route being injected into the N2N architecture. At each physical ingress and egress of the HSGR's ATM interface will be an Edge suite that consists of a firewall, Intrusion Protection System (IPS) and Edge Router.

#### **2.6.15.3 FAILURE OF THE DISN SERVICE AT THE IT-21 FLTNOG (FAILOVER)**

In the event of a DISN failure, or major service outage, all services will be redirected to the failed IT-21 FLTNOG Fleet Router, through the HSGR, to the backup IT-21 FLTNOG Fleet Router. As an example, UAR IT-21 FLTNOG ships will appear as if

they are a PR IT-21 FLTNOC ship and will continue to receive all IP services via the PR IT-21 FLTNOC. The failover process is transparent to the Fleet customers and no intervention is required by the users.

Figure 2-13 shows an example of a DISN failure at UARNOC.



**Figure 2-13**  
**DISN failure at UARNOC**

**2.6.16 CLASSIFIED TRUSTED NETWORK PROTECTION POLICY (CTNPP)  
/ UNCLASSIFIED TRUSTED NETWORK PROTECTION POLICY (UTNPP)**

The Navy Classified Trusted Network Protection Policy (CTNPP) and the Unclassified Trusted Network Protection Policy (UTNPP) provide Navy enclave protection to reflect a defense-in-depth measure and the minimum standards for interconnection between Navy trusted networks (networks which comply with UTNPP/CTNPP) and untrusted networks. NTD 09-07 refers.

**2.6.17 IP VERSION (IPV6)**

Internet Protocol Version 6 (IPv6) is the next generation network layer protocol of the Internet as well as the GIG, including networks such as NIPRNET, SIPRNET, JWICS, and emerging DoD space and tactical communications systems. Implementation of IPv6 is necessary due to the fundamental limitations of the current Internet Protocol, Version 4 (IPv4) protocol, including a maximum of only 4,294,967,296 possible IP addresses (of which, almost 300 million are reserved for special purposes). An IP address is a unique address that computers, routers and switches use to communicate on a network. In its present form, IPv4 cannot support the long-term requirements of both the DoD and the commercial community. IPv6 overcomes these limitations by expanding the available IP address space to accommodate the worldwide explosion in Internet usage. This improves end-to-end security, facilitates mobile communications, provides new enhancements to Quality of Service (QoS), and eases management system burdens. Additionally, IPv6 is designed to run well on most modern high-speed networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) without experiencing significant decreases on low bandwidth systems. IPv6 also greatly expands the number of available unique IP addresses available for use and eliminates the need for complex address conservation methods such as Classless Inter-domain Routing (CIDR).

**2.6.18 GLOBAL COMMAND AND CONTROL SYSTEM - MARITIME (GCCS-M)**

GCCS-M is the maritime implementation of the joint services GCCS providing a single, integrated, scalable C4I system. The system supplies information that aids Navy commanders in a full range of tactical decisions. In functional terms, GCCS-M fuses, correlates, filters, and maintains raw data and displays image-building information as a tactical picture. Specifically, the system displays the location of air, sea, and land units anywhere in the world and identifies whether those units represent friendly, neutral, or enemy forces. It operates in NRT and constantly updates unit positions and other SA data. GCCS-M also records the data in appropriate databases and maintains a history of the changes to those records. The user can then use the data

individually or in concert with other data to construct relevant tactical pictures, using maps, charts, map overlays, topography, oceanographic, meteorological, imagery, and all-source intelligence information all coordinated into what is known as a CTP that can be shared. Supplied with this information, Navy commanders can review and evaluate the general tactical situation, determine and plan actions and operations, direct forces, synchronize tactical operations, and integrate force maneuver with firepower. The system operates in a variety of environments and supports joint, coalition, and allied forces.

The GCCS-M architecture is composed of three variants: GCCS-M afloat, GCCS-M ashore, and GCCS-M tactical/mobile that includes TSCs, mobile operations control center (MOCC), and Joint Mobile Ashore Support Terminal (JMAST).

## **2.7 VOICE AND VIDEO SERVICES**

### **2.7.1 VOICE OVER IP (VOIP)**

The mission of the Satellite Management Branch (Standardized Tactical Entry Point) and the Teleport Program Office (TPO), and Readiness Contingency and Exercise Support Branch is to extend Defense Information System Network (DISN) services to Joint Forces worldwide using both terrestrial and satellite communications (SATCOM). DISA's goal is to put a net-centric Internet Protocol (IP) architecture in place to better support the Warfighter. An individual DoD Gateway site is intended to be the interface between the deployed users and the Defense Information Systems Networks (DISN). IP based solutions are intended to enhance the DoD Gateways capabilities not replace legacy DISN services. To meet today's IP based solution shift, initial IP based solution suites have been installed at Landstuhl, Germany, Camp Roberts, California, and Fort Monmouth, New Jersey. The IP based solution suite supports SIPRNET (Secret Internet Protocol Router Network, NIPRNET (Unclassified but Sensitive Internet Protocol Router Network), Voice over IP (VoIP), JWICS, DRSN, Commercial ISP, and Commercial Voice applications. These emerging IP based solution exploit both traditional FDMA SATCOM modems and IP SATCOM Modems (current force and Joint Internet Protocol Modem (JIPM)) for long haul transport. The individual requirements are numbered to aid in tracking and for cross-referencing between the segment specifications, the system specification, and the Teleport Operational Requirements Document. The numbering system uses a designator in the following format: BXXXX, in which B is a letter defining the system or segment and the Xs represent numerals. The current conceptual the Teleport IP based solution equipment is annotated. The design incorporates three main new elements into the existing baseband architecture and new equipment to the encryption element: a convergence element (also known as the convergence router), a VoIP functionality (also known as the VoIP

gateway), a performance enhancing proxy (PEP) element, and a High Assurance Internet Protocol Encryption (HAIPE). HAIPE devices provide traffic separation and COMSEC functionality.

The convergence router will bring together NIPRNET, SIPRNET, and DSN VoIP traffic into a packet stream. The aggregate of the convergence router can be sent to either to the Multiplex Integration and Digital Communications Satellite Subsystem Automation System (MIDAS) or the IP SATCOM Modem. MIDAS will then transmit the Convergence Router traffic to the STEP/Teleport System's transmission security (TRANSEC) element. From the TRANSEC element, the MIDAS connects to the FDMA modem for transmission via satellite. The IP SATCOM Modem will support IP over Transponded SATCOM as well. The TRANSEC solution for IP SATCOM Modem employment is still not defined. The deployed warfighters' suite of equipment will reverse the convergence process, using similar equipment, by means of interoperable routing protocols and encryption keys for TRANSEC and communications security (COMSEC). The Encryption Element provides the TRANSEC and COMSEC required by the Gateway Systems. All satellite transmissions require TRANSEC in accordance with CJCSI 6510.01D, Information Assurance (IA) and Computer Network Defense (CND). COMSEC will be applied to all tactical circuits requiring COMSEC. The DoD Gateway System does not support unencrypted data above the Secret level; for example, JWICS and DRSN data passes through the systems encrypted. The interconnection element provides the electrical and physical interface between most elements of the DoD Gateway. It supports connectivity to either serial interface from the convergence router to the encryption element for TRANSEC or Ethernet connection into a IP SATCOM Modem. The modem element provides both FDMA modems and IP SATCOM Modems (TDMA) interfacing with the DoD Gateway terminal equipment for transmission over the satellite to the warfighter. The modems provide the needed modulation and demodulation for the SATCOM link. The VoIP gateway will be used to interface with the DSN and to convert legacy DSN voice to VoIP. The VoIP traffic will be sent to the convergence router to be merged with the NIPRNET and SIPRNET traffic.

B1190—The VoIP gateway shall support IPv4.

B1200—The VoIP gateway shall support IPv6 or have a migration plan to implement IPv6 in future releases.

B1210—The VoIP gateway shall support QoS and CoS. All DoD Gateways will adhere to defined DISN CORE CoS and QoS standards and policies.

B1220—If no DoD policy with respect to QoS and CoS has been established, the VoIP gateway QoS and CoS shall comply with tactical user configurations.

### **2.7.2 DOD VIDEO TELECONFERENCING SERVICE (VTC)**

VTC is an extension of traditional telephony technologies with the added feature of being able to see the person or persons with

whom one is talking. Another way to consider VTC technology is an extension or combination of television, which provides the audio and video communication aspect, and telephony or telecommunications which provides the addressable, bi-directional connectivity. The results of which are a bi-directional, "closed circuit", dial-able, TV system. The television portion of the technology uses video display screens (televisions/video monitors/projectors), video cameras, microphones, and speakers at each location connected to a Coder-Decoder (CODEC). The CODEC is the interface between the analog voice/video devices in the system and the addressable connectivity or transmission portion of the system. The CODEC converts the analog signals to digital format that is compatible with the transmission media. The CODEC also interfaces and converts presentation and whiteboard information. The combined digital signal is then transmitted to the remote location via a telecommunications network which is either TDM or IP based. Quality VTC communications requires much higher bandwidth than voice or traditional data communications. The actual bandwidth required is dependent upon the CODEC and compression algorithm used. The typical minimum bandwidth requires is 128Kbps with 384Kbps being typical and required for quality video. Some CODECs require as much as 2Mbps in support of high definition video.

The telecommunications network used for VTC connectivity is a traditional circuit switched telephony network such as the Defense Switched Network (DSN) and/or Public Switched Telephone Network (PSTN). The DSN is the preferred network for DoD VTC connectivity. Both of these networks are based in TDM technologies and typically provide Integrated Services Digital Network (ISDN) lines for access to the network. Both Basic Rate interface (BRI) and Primary Rate interface (PRI) ISDN lines are used. Addressability is handled as with any other telephone instrument, the address is the phone number associated with the line from the circuit switch to the instrument.

### **2.7.3 DEFENSE SWITCHED NETWORK (DSN)**

The Defense Information System Network (DISN) provides global voice services through the Defense Switched Network (DSN), a worldwide private-line telephone network. Multilevel precedence and preemption (MLPP) capabilities on the DSN utilized by command and control users ensure that the highest-priority calls achieve connection quickly, especially during a crisis situation. The DSN also provides global data and video services using dial-up switched 56Kbps or 64Kbps Integrated Services Digital Network (ISDN) services. Secure voice services are provided by the Secure Telephone Unit, Third Generation/Secure Terminal Equipment (STUIII/STE) family of equipment that provides end-to-end encryption over non-secure DSN circuits. Interfaces are provided between strategic and tactical forces, allied military and Enhanced Mobile Satellite Services (EMSS).

#### **2.7.4 DEFENSE RED SWITCH NETWORK (DRSN)**

The Defense Information System Network (DISN) provides global secure voice services using the Joint Staff Defense Red Switch Network (DRSN). The Joint Staff grants approval to access the network. The mission of the DRSN is to provide the President, Secretary of Defense, National Command Authority (NCA), the National Military Command Center (NMCC), Combatant Command Centers, Warfighters, and other critical Department of Defense and federal government agencies with reliable, secure, interoperable C2 and crisis management capabilities.

#### **2.7.5 INTEGRATED SERVICES DIGITAL NETWORK (ISDN)**

ISDN is a circuit-switched telephone network system, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher data speeds than are available with analog. More broadly, ISDN is a set of protocols for establishing and breaking circuit switched connections and for advanced call features for the user.

#### **2.7.6 PLAIN OLD TELEPHONE SYSTEM (POTS)**

POTS refers to an un-enhanced telephone service with the ability to send and receive phone calls. In POTS, once a dedicated circuit connects the call, your voice is transmitted by a 4kHz analog wave form via a process known as a frequency division multiplexing. 4kHz band is used because it provides enough bandwidth to reproduce a recognizable human voice. Further, each channel supports a range of single amplitude (strength) that relates to a volume level. The amplitude level is limited, so no matter how loud you scream over the network it won't exceed a certain volume on the other end of the line. Together this combination of bandwidth and amplitude is not quite enough for perfect voice transmission, but is good enough so you can make out the words and recognize familiar voices.

#### **2.7.7 AFLOAT PERSONAL TELECOMMUNICATIONS SYSTEMS (APTS)**

Providing personal telecommunications service to shipboard crewmembers at sea is a highly visible quality of life issue that positively affects the life of the sailor at sea. To maintain clear separation of appropriated and non-appropriated activities, SPAWAR and Navy Exchange Command (NEXCOM) work collaboratively to insure that the definition of technical and procedural requirements do not conflict in planning for future commercial services. This clear separation of functionality and funding is



known as the APTS system. With a fully complemented CV/CVN, costs per minute have driven down phone call charges into the \$1.00 per minute range. A commercial smart debit card now provides telephone services for personnel on most ships equipped with the APTS "Sailor Phones".

#### **2.7.8 KY68 DIGITAL SUBSCRIBER VOICE TERMINAL (FDVT)**

KY68 is a ruggedized field terminal containing the audio processing, signaling and Communications Security (COMSEC) functions necessary to provide secure and non-secure voice and secure data access to circuit switched digital networks, and to provide secure access to a variety of non-switched, point-to-point (sole user) digital networks. The TSEC/KY-68 DSVT digitizes voice information using Continuously Variable Slope Delta (CVSD) modulation at a 16 or 32Kbps rate. The KY-78 is the strategic version.

#### **2.7.9 VIDEO INFORMATION EXCHANGE SYSTEM (VIXS)**

The video information exchange system (VIXS) provides a secure, GENSER SECRET and SCI, multipoint, interactive video teleconference (VTC) capability that facilitates efficient communications among CNO, fleet commanders, commanders at sea, Navy and Marine Corps fleet command authorities, and other users. It was originated in 1992 as CNO VTC and expanded to the fleet flagships in 1993. In 1994 the name was changed to VIXS and it expanded to include CVs, CVNs, and large deck amphibious ships, LHAs and LHDs. VIXS was implemented with COTS VTC systems and multipoint control units (MCUs) (bridging units) and utilizes Navy-standard cryptographic equipment. This integrated system supports global tactical C2 requirements to conduct distributed, collaborative planning.

Through the use of compressed digital transmission, the system provides a cost-effective means of producing high-quality video images using reduced bandwidth. VIXS conferences are normally held at 128-256Kbps. This reduced bandwidth requirement minimizes the expense of long distance service to Europe and allows SATCOM connectivity to Navy ships at sea. Normal shipboard bandwidth is 128 kbps, but CWSP gives equipped ships the bandwidth required to conference at 256 or 384Kbps. Live motion video, camera auto queue on speaker, computer graphics, videotape, document images, white boarding, and file sharing can currently be transmitted over the system. Support can be provided for up to 16 conferencing sites, enabling 8 simultaneous point-to-point conferences, or a series of mixed point-to-point and multipoint conferences. Gateways located at MCU sites provide access to other networks.

VIXS hubs are located at:

1. NCTAMS LANT Norfolk, VA
2. NCTS NAPLES, ITALY Naples, Italy
3. NCTAMS PAC Makalapa, HI
4. NCTS Bahrain.

VIXS shore access is provided to COMPACFLT, USPACOM, CFFC, United States Joint Forces Command (USJFCOM), COMUSNAVEUR London and Naples, NAVCENT Bahrain, and CNO. An additional 30 plus sites have been certified as VIXS network users via ISDN dial-up. A support hub at Space and Naval Warfare (SPAWAR) Systems Center (SSC) Charleston provides testing and diagnostics support in addition to providing backup multipoint conference support. The VIXS shipboard configuration consists of one suite of VTC hardware and two separate encryption paths. One path is classified (GENSER) and the other is JWICS SCI. Both paths are encrypted via a KG-194 or KG-194A.

In FY02, upgrades included incorporation of a second MCU at VIXS hub sites to support simultaneous local unclassified and/or NATO multipoint conferences. Future hub upgrade requirements will include support of IP based systems such as adding an H.323 MCU and H.320/H.323 Gateway to accommodate NMCI user sites as well as adding additional port capacity to the Madge and Montage units to accommodate additional afloat and ashore VIXS users. Additional afloat platforms are expected to include CG and DDG utilizing SHF.

#### **2.7.10 DISN VIDEO SERVICE GLOBAL (DVSG)**

DVS-G capabilities include global connectivity, 24/7 availability, multiple security levels (Unclassified, U.S. Secret, and TS), and VTC services via STEP sites. VTC services are provided using multiple configurations (point-to-point, multi-point, switched, or dedicated), speed matching, and bridging services. If C2 capabilities are required, DVS-G must be configured to meet C2 performance measures.

DISA is planning to transition DVS-G to DVS II, a new IP-based network that includes C2 VTC operations. DISA is developing the follow-on DVS II contract; however, implementation dates are not presently available. The follow-on contract requirements include many new technologies, the merging of existing networks, and advanced connectivity to the warfighter. DVS II will build on the DVS-G platform.

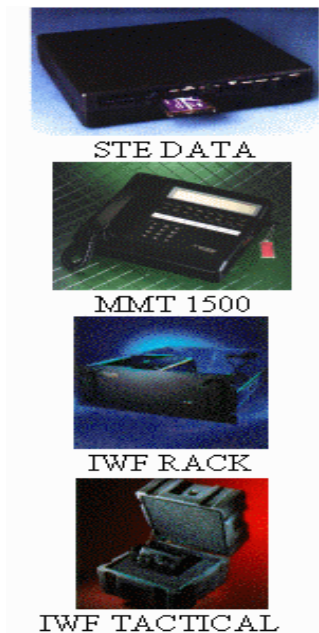
The DISN Video Services (VS) provides global DOD VTC users a bridging service using industry standard technology for interoperability and multi-point VTC requirements for both classified and unclassified users. Increased flexibility was added to the system by providing subscribers a way to access VTC users on tactical networks such as the DSCS and DSN, as well as non-DOD networks. Through a cascade of Multipoint Control Units (MCU), DISN VS allows subscribers to access customer MCUs such as the Navy's tactical Video Information Exchange System (VIXS).

DISN VS supports Top Secret bridging requirements, providing VTC services to all U.S. Forces deployed worldwide. Additionally, through a processing procedure DISN VS supports Allied conferencing up to and including Top Secret. Existing DISN VS capabilities include global connectivity, multiple levels of security, reservation scheduling, directory assistance, multi-point conferencing, speed matching, access via STEP, and 24/7 help desk accessibility. Use of DISN VS is available through either dedicated service or dial-up (switched) service.

### 2.7.11 STE / STU (SECURE TELEPHONE)

Secure Telephone Unit - Third Generation (STU-III) is a low-cost, user-friendly, secure telephone device. The terminals are designed to operate reliably, with high voice quality, as both ordinary telephones and secure instruments over the dial-up public switch telephone network. STU-III operates in full-duplex over a single telephone circuit using echo canceling modem technology. STU-IIIs come equipped with 2.4 and 4.8Kbps code-excited linear prediction (CELP) secure voice. Secure data can be transmitted at speeds of 2.4, 4.8, and 9.6Kbps. There are many manufacturers each having different maximum throughput rates. The data throughput between two STU-IIIs can only be as great as the slowest STU-III connected.

The STU-III Family consists of some of the following devices (see figure 2-14):



**Figure 2-14**  
**SECURE VOICE EQUIPMENT**

1. The STU-III/Low Cost Terminal (LCT) was designed for use in the office environment among a broad spectrum of military, civil, government, and selected private sector users. It is compatible with standard modular or multi-line (key system) connectors and operates full-duplex over a single telephone circuit.
2. The STU-III/Cellular Telephone is interoperable with all other versions of the STU-III Family. It combines cellular mobile radiotelephone technology **with** advanced secure voice/data communications. The unit includes a message center that is integrated with the standard cellular handset; it can be conveniently mounted inside a vehicle and provides all STU-III functions, including authentication/classification display.
3. The STU-III/Allied (A) is a specialized version of the STU-III/LCT that is compatible with the STU-II. It retains all basic STU-III functions and capabilities and incorporates STU-II BELLFIELD Key Distribution Center (KDC), STU-II net, and STU-II multipoint modes of operation.
4. The STU-III/Remote Control Interface (RCU) provides RED enclave subscribers with STU-III compatible secure communications in a rack-mounted remotely controlled line encrypting unit. When used in conjunction with a RED switch or conferencing director, the STU-III/R allows STU-III users to confer with multiple STU-III users or others who have secure functions. It is capable of encrypting/decrypting voice or data over two-wire or four-wire telephone systems and incorporating a 2.4Kbps BLACK digital (external modem) interface.
5. The Multi-Media Terminal (MMT) 1500 is a diversified STU-III capable of clear or secure voice and data communications over both analog and digital mediums. The MMT interfaces to the commercial telephone system via a standard RJ-11 telephone jack and to digital systems through a Black Digital Interface (BDI). The BDI port will support both half-and full-duplex communications, precedence dialing, black digital network signaling, and multiple satellite hops. When unattended the MMT can automatically answer an inbound call without operator intervention and establish a secure link with any user on a preprogrammed Access Control List (ACL).
6. The Inter Working Function (IWF) is the shore gateway device that provides the digital to analog conversion between the MMT and the analog STU-III. The IWF supports half and full duplex voice and data communications with rates of 2.4, 4.8, and 9.6Kbps. The IWF improves secure voice and data synchronization over multiple satellite hops with programmable extended time-outs and pre-staging of STU-III call information. The IWF supports all necessary network-signaling functions to enable call setup and status messages including canned voice messaging to the analog user.

7. The STU-III Secure Data Device (SDD) is designed with the same capabilities as other members of the STU-III family including Secure Access Control System (SACS), remote authentication (RA), remote control, auto-answer secure data, and capable of operating in both attended and unattended environments. The SDD provides protection for facsimiles, e-mail, and computer communications.
8. The Motorola CipherTAC 2000 (CTAC), (see figure 2-15) STU-III family compatible secure voice communications via cellular phone. CTAC without an inserted CipherTAC 2000 security module is unclassified and functions as a non-secure commercial off the shelf (COTS) telephone product. The CTAC CipherTAC security module is certified for all levels of classified discussions up to and including SECRET in an adequate operating/security environment.



**Figure 2-15**

#### The Secure Terminal Equipment (STE)

The Secure Terminal Equipment (STE)/Office is the evolutionary successor to the STU-III. The STE program will improve shore secure voice communications as well as shipboard communications by changing out the analog STU-III products with digital-based STE products. The STE cryptographic engine is on a removable Fortezza Plus KRYPTON™ Personal Computer Memory Card International Association (PCMCIA) Card, which is provided separately. The STE Data Terminal provides a reliable, secure, high rate digital data modem for applications where only data transfer (FAX, PC files, Video Teleconferencing, etc.) is required. All STE products will be STU-III secure mode compatible with the following enhanced capabilities:

1. Voice-recognition quality secure voice communication.
2. High-speed secure data transfers (up to 38.4Kbps for asynchronous or 128Kbps for synchronous).

STE terminal products can use Integrated Services Digital Network (ISDN), analog PSTN, TRI-TAC, or direct connection to Radio Frequency (RF) assets via RS-530A/232E ports. Maximum STE performance may be attained only by those commands employing ISDN service with two Bearer Channels (2B+D ISDN Service). When connected to a PSTN (Analog Telephone) service, the STE/Office units will only support current STU-III voice and data capabilities.

A tactical version, STE/Tactical is a replacement for MMT 1500

with a Digital Non-secure Voice Terminal (DNVT) adapter. Though not a direct replacement for the KY-68, the STE/Tactical can serve as a DNVT replacement with secure voice communication capabilities in STU-III modes over TRI-TAC/Mobile Subscriber Equipment (MSE). STE/Tactical is not secure mode compatible with the Digital Secure Voice Terminal DSVT KY-68.

A STE Direct Dial capability comprised of the STE/C2 Tactical terminal and/or associated STE/Interworking Function(s) will improve on the existing Navy "Direct Dial" secure voice ship to shore dial-up operations. STE Direct Dial improves secure mode connectivity, provides operational flexibility support for both plain text and cipher text voice modes, and provides a standardized secure ship digital telephone system solution and Joint CINC interoperability with forces at sea and ashore.

Individual STE Product Capabilities:

1. STE/Office provides enhanced STE capabilities over digital ISDN and STU-III over analog PSTN.
2. STE/Data provides STE and STU-III data capabilities only.
3. STE/Tactical with Wedge supports STU-III Black Digital Interface (BDI) over TRI-TAC/MSE or RF asset.
4. STE Direct Dial:
  - a. STE/C2 Tactical with Wedge supports STU-III BDI over ISDN or RF asset.
  - b. STE/IWF provides interface with PSTN (Analog) and ISDN (Digital).

STE products without an inserted Fortezza Plus KRYPTON™ Card are unclassified and function as non-secure COTS telephone products. The Fortezza Plus KRYPTON™ Card is currently designated as an Accounting Legend Code 1 (ALC-1) item by the NSA. Even though STEs are unclassified items, they should still be treated as high-value Government property (e.g., such as an office computer). Certification of STE will provide security for all levels of traffic, up to and including TOP SECRET Special Compartmented Information (TS-SCI). When a Fortezza Plus KRYPTON Card is inserted into a STE, secure storage must be provided to the extent required by SECNAV M5510.36 (series) for the maximum classification level of the key used. Fortezza Plus KRYPTON™ Card is considered classified to the maximum level of key classification until it is associated with a STE terminal. Once associated with a STE terminal, the card is considered unclassified when not inserted in the associated STE terminal.

### 2.7.12 ADVANCED NARROWBAND DIGITAL VOICE TERMINAL (ANDVT)

The Advanced Narrowband Digital Voice Terminal (ANDVT) Family comprises the AN/USC-43 Tactical Terminal (TACTERM), the KY-99A Miniaturized Terminal (MINTERM), and the KY-100 Airborne Terminal (AIRTERM). These terminals are handled as UNCLASSIFIED controlled cryptographic items (CCIs) when unkeyed; when keyed they assume the classification of the key. The ANDVT family provides joint interoperability between Service components of US command elements and North Atlantic Treaty Organization (NATO) allies.

ANDVT Family units are primarily used to satisfy tactical secure voice requirements on high frequency (HF), very high frequency (VHF), and ultra high frequency (UHF) satellite and line-of-sight (LOS) communications; UHF Non-Demand Assigned Multiple Access (Non-DAMA) and DAMA; super high frequency (SHF) and extremely high frequency (EHF) satellite communications (SATCOM) including Milstar; UHF Follow-on (UFO)/EHF; and Fleet Satellite EHF Package (FEP). All ANDVTs must have engineering change proposal-060 (ECP-060)/field change -1 (FC-1) incorporated in order to operate over UHF SATCOM.

**TACTERM:** The TACTERM normal configuration consists of the Basic Terminal Unit (BTU) (CV-3591) and a communications security module (KYV-5), providing half-duplex, secure transmission of voice or data communications in either point-to-point or netted mode. The peripherals include the split remote control units (SRCUs) Z-ANG and Z-ANH, which replaced the existing PARKHILL type IIIA and IIIB. A "Y" cable will allow remote loading of cryptographic variables from the SRCU Z-ANG. The Navy developed the TACTERM in association with the National Security Agency (NSA). See table 2-1 for a listing of some TACTERM Equipment.

**MINTERM:** The functions of the MINTERM are similar to those of the TACTERM; however, its updated design includes an improved modular architecture, and it has been reduced in size. The MINTERM is a low-cost, lightweight, low-power single channel, half-duplex, narrowband/wideband/wireline terminal providing secure voice and data communications with full key distribution and remote rekey capabilities. The MINTERM is certified to secure traffic up to TOP SECRET.

The MINTERM improvements include the following:

- a. Concurrent voice and data modes enable the users to connect both data equipment and voice handsets.
- b. VINSON (KY-57/58) mode of operation allows interoperability between the MINTERM and the VINSON wideband COMSEC equipment.
- c. Improved SATCOM performance incorporates the enhancements included in ECP-060/FC-1 to the ANDVT. This includes an extended preamble for improved synchronization, selectable receive (RX) or transmit (TX) priority to prevent transmission conflicts,

Milstar mode requirements, push-to-talk (PTT) inhibit, and a bridge for signal fades.

The latest DOD LPC-10 algorithm (V58) has been enhanced to provide high-quality secure narrowband voice for military handsets and to maintain that quality and intelligibility in noisy acoustical environments.

**AIRTERM:** NSA is developing AIRTERM. Although originally designed for airborne applications, the Navy has also identified submarine, shipboard, Marine Corps communication vans, and landing craft air cushion (LCAC) requirements. AIRTERM incorporates MINTERM and VINSON operational modes. It is a wideband/narrowband terminal that interoperates with the TACTERM, MINTERM, VINSON, and Single Channel Ground and Airborne Radio System (SINGARS). The AIRTERM is a lightweight, self-contained secure voice and data terminal that provides secure half-duplex voice, digital data, analog data, and remote-keying capabilities for transmission over radio circuits or wire line media. AIRTERM accepts classified analog voice information and uses advanced speech processing algorithms: LPC-10 at 2.4Kbps in narrowband voice modes and continuously variable slope delta (CVSD) modulation at 12Kbps and 16Kbps in wideband voice modes. The AIRTERM provides the same connectors, with similar functional pin outs, as the VINSON for the wideband operational modes. The AIRTERM is also available with a remote control unit (RCU), Z-AVH, which is functionally equivalent to the Main Terminal Unit (MTU) with regard to external controls.

**Characteristics:**

Equipment	Height (in)	Width (in)	Depth (in)	Weight (lb)
CV-3591	7.63	4.91	13.30	21.80
KYV-5	6.25	4.88	3.00	3.60
Z-ANG (SRCU)	2.25	5.72	4.13	3.30
Z-ANH (SRCU)	6.20	6.91	2.97	3.30
KY-99A	3.00	5.50	6.73	4.50
KY-100	4.96	5.73	5.14	5.70
Z-AVH	2.61	5.73	3.14	1.80

**Table 2-1**  
**TACTERM EQUIPMENT**



Supports the following Data Rates:

Narrowband (3kHz) 300 bps, 600 bps, 1200 bps, and 2400 bps in the HF mode

2400 bps digital secure voice in the HF mode

2400 bps digital voice and data in the LOS mode

#### **MINTERM**

Supports the following Data Rates:

Narrowband (3 kHz) 300, 600, 1200, 2400 bps in HF or BLACK digital mode (BDM)

2400 bps in LOS mode

Wideband (25 kHz) 12 and 16 kbps in the VHF/UHF/SATCOM mode

#### **AIRTERM**

Supports the following Data Rates:

Narrowband (3 kHz) 300, 600, 1200, 2400 bps in HF or BDM

2400 bps in LOS mode

2400 bps digital secure data in the LOS mode

Wideband (25 kHz) 12 and 16 kbps voice or data in the baseband/diphase (BB/DP) mode

### **2.7.13 FUTURE NARROWBAND DATA TERMINAL (FNBDT) STANDARD**

NSA achieved secure interoperability between some wired and wireless systems when it created an industry and government consortium that agreed on a common signaling protocol called the Future Narrow Band Digital Terminal (FNBDT). Despite its name, however, FNBDT is no longer just narrow band, but also includes a common voice processing capability, a crypto-algorithm base and a key-management process. It has become the primary security standard for cell phones, military radios and emerging public safety communications devices for homeland security missions and first responders around the world. FNBDT products were designed to accept—and have accepted—secure software upgrades. For example, the General Dynamics Sectera Secure GSM phone as well as the Qualcomm QSec-800 CDMA secure cell phone, have added upgrades that provide the ability to pass short messaging data.

Although the data file transfers are limited to low bandwidth, the addition of secure voice and data interoperability in FNBDT mode is a first step toward the convergence of voice and data over secure wireless networks. NSA now maintains an FNBDT interoperability test bed that verifies vendor compliance with the current version of FNBDT specifications and tests interoperability among the current versions of all wireline and wireless products to verify secure, end-to-end interoperability.

## 2.8 INTELLIGENCE AND CRYPTOLOGIC SYSTEMS

### 2.8.1 JOINT SERVICES IMAGERY PROCESSING SYSTEMS (JSIPS-N) CONCENTRATOR ARCHITECTURE (JCA)

Imagery is the highest use of bandwidth for the CSG or ESG, typically on the order of 768Kbps. The JSIPS JCA was developed for the fast and efficient delivery of imagery while providing increased flexibility in bandwidth management. The JCA is a client-server based architecture, with web-like browsing features and capabilities for fleet imagery subscribers that is scalable up to 8Mbps. It provides the fleet with a SECRET, GENSER, user-friendly network-centric, imagery delivery system. The JCA has four major components, including imagery sources, concentrators, sites, and communications.

1. Imagery sources – Sources originate imagery and imagery-related products that are required by users for various operational needs such as tactical reconnaissance, battle damage assessment (BDA), and targeting.
2. JCA concentrator – The primary concentrator is the JCA central repository of imagery and imagery related products that are supplied to the fleet. The data comes from the source, and populates databases based on standing fleet imagery requirements as well as individual fleet-initiated requests for imagery and imagery-related products.
3. JCA sites – Navy afloat JCA sites are command ships, carriers, and large deck amphibious ships (LHD/LHA). Each site houses an image product library (IPL) workstation that is used to coordinate delivery, ordering and acknowledging receipt of imagery products.
4. JCA communications – Communications between the concentrator and ESG and CSG ships are via broadband (DSCS or CWSP) SATCOM connectivity.

### 2.8.2 GLOBAL COMMAND CONTROL SYSTEM - INTEGRATED INTELLIGENCE AND IMAGERY

Global Command and Control System-Integrated Intelligence and Imagery (GCCS-I3) provides COP-centric imagery and intelligence-related capabilities developed by the four military services and selected agencies in response to joint warfighter requirements. Through the GCCS-I3 integration process, these tools provide intelligence support to operations seamlessly within the GCCS family of systems.

GCCS-I3 enhances the operational commander's situation awareness by providing a standard set of integrated, linked tools and

services that give ready access to imagery and intelligence directly from the operational display. GCCS-I3 gives tactical operators and intelligence analysts' direct access to the nationally produced modernized integrated database (MIDB) for order of battle (OOB) data, weapons systems characteristics and performance information, and national imagery. GCCS-I3 also gives those users the capability to integrate locally collected tactical imagery, live video stream, and other intelligence with national and theater-produced intelligence. This intelligence can be plotted directly on operational/tactical displays alongside continuously updating operational and operational-intelligence information, providing tactical operators and intelligence analysts vastly improved knowledge of the tactical battlespace. The all-source fusion capabilities of GCCS-I3 provide decision makers with a composite picture of the battlespace augmented with SCI-level intelligence, bringing together NRT track, OOB, maps and imagery, military overlays, and other forms of specialized intelligence data to produce a CIP. When combined with other enabling technologies, such as database replication and guards, GCCS-I3 supplies geographically focused, OPINTEL to the GCCS-M CTP battlespace view, aiding decision support and improved SA for the intelligence and operations elements of the commander's staff.

Included in the GCCS-I3 suite are the following applications:

1. Joint threat analysis tools/ground template toolkit (JTAT/GTT) generates terrain suitability and other tactical decision aids based on military aspects of terrain and contributes to intelligence preparation of the battlespace (IPB) analysis. It supports the joint force and component commanders' campaign/mission planning and decision making by identifying, assessing, and estimating the adversary's battlespace center of gravity, critical vulnerabilities, capabilities, limitations, and intentions, most likely COA, and COA most dangerous to friendly forces.
2. Joint targeting toolbox (JTT) provides a common standardized, scalable, and DII-COE compliant set of targeting tools to manage and/or produce targets, target data, and target-derived products and services in response to customer requirements in a manner consistent with targeting mission objectives and warfighter requirements.
3. Improved many-on-many (IMOM) models electronic combat scenarios and can provide threat evaluation. It is a 2-D graphics oriented user-interactive program which aids in mission planning and IPB analysis. IMOM visually displays the complex interaction of multiple ground-based radar systems being acted upon by multiple airborne ECM aircraft. IMOM models the detection capabilities of radar effects, the effects of stand-off jamming platforms, and the effects of self-protection jamming platforms. The model adds the effects of terrain masking and ECM on any OOB, exploits the results to perform a variety of analyses, and provides hard copy post processing in a variety of formats.

### 2.8.3 JOINT DEPLOYABLE INTELLIGENCE SUPPORT SYSTEM (JDISS)

The Joint Deployable Intelligence Support System (JDISS) program provides a family of hardware and software capabilities that allow connectivity and interoperability with intelligence systems supporting forces, in garrison, and deployed during peace, crisis, and war. It provides the Joint Intelligence Center (JIC), Joint Task Forces (JTF) and operational commanders with on-site automation support and the connectivity necessary to execute the intelligence mission. JDISS and the Joint Worldwide Intelligence Communications System (JWICS) together comprise the joint standard and foundation for commonality among intelligence support systems. JDISS provides joint intelligence centers, joint task forces, and operational commanders with on-site automation support and the connectivity to make the best use of the Intelligence Community's resources. JDISS is also the technical baseline for DODIIS client-server environment (CSE).

JDISS provides automated support for the following:

1. transmitting and receiving specific requests for intelligence
2. Accessing Theater, Service and National intelligence databases
3. Supporting digitized imagery exchange
4. Accessing automated record message processing systems, indications and warning systems, and collection management systems
5. Inputting intelligence data into a variety of operations/intelligence systems, and
6. Performing multi-media functions, such as voice electronic publishing and video teleconferencing.

The core software for JDISS is:

1. E-mail/chat
2. Word processing/message generator
3. Imagery manipulation
4. Communications interfaces/map graphics
5. Briefing tools/utilities, and
6. Desktop video/voice

JDISS can be utilized in any context which requires the connectivity and interoperability with the intelligence systems. This product has been accepted as part of the GCCS suite of products. This means that the experts from the GCCS Executive Agent have created and evaluated the quality and applicability of this product for use within the GCCS domain for the Department of Defense.

## 2.8 4 TACTICAL EXPLOITATION SYSTEM - NAVY

Tactical exploitation system-Navy (TES-N) is the Navy shipboard implementation of the Army tactical exploitation system (TES-A). TES-N is presently installed only on PAC Fleet CVNs. It is an integrated, scalable, multi-intelligence system specifically designed for rapid correlation of national and theater ISR information to support network-centric operations. TES-N provides the warfighting commander with access to NRT, multi-source, and continuously updated day/night battle space ISR information. TES-N supports strike operations using numerous ISR collection planning, data correlation, geo-location, data dissemination, and storage functions.

It is interoperable with other service derivatives of the TES system: TES-A, the Marine Corps' tactical exploitation group (TEG), and the Air Force's ISR manager.

## 2.8 5 INTEGRATED BROADCAST SYSTEM

IBS has integrated several existing intelligence and information dissemination systems into a single system of broadcasts that will allow for the receipt of data via a single receiver (the joint tactical terminal). IBS will disseminate threat avoidance, targeting, maneuvers, force protection, target tracking, and target/situation awareness information, and will be continuously refined by data from national, theater, and tactical sensors. The reported information will contain unique references (e.g., report or track/event number) to allow IBS producers and users to correlate IBS products. IBS will allow the tactical user to construct successively detailed intelligence pictures of the battlespace. IBS will interface with Tactical Data Links (TDLs) such as Link 16 and joint variable message formats (VMFs) networks to ensure a seamless flow of intelligence information onto those networks.

The IBS architecture will be theater-based dissemination with global connectivity through terrestrial and high capacity communications paths. IBS will take advantage of the communications paths users already have by implementing an information management scheme integrated with other DOD information management systems (e.g., GBS information dissemination manager).

The effective dissemination of NRT intelligence data requires secure, worldwide data communications with prioritized use of available bandwidth between producers and users at all echelons of command. The existing components of the IBS are:

1. Simplex (IBS-S) - formerly known as the TRAP data dissemination system (TDDS).

2. Interactive (IBS-I) – formerly known as the tactical information broadcast service (TIBS).
3. Network (IBS-N) – formerly known as the NRT dissemination (NRTD) system.
4. LOS (IBS-LOS) – formerly known as the Tactical Reconnaissance Intelligence eXchange System (TRIXS).

Additionally, TADIXS-B is currently part of the overall IBS network but will not migrate into the final IBS architecture. The legacy intelligence dissemination systems were developed to support the operational requirements of specific groups of users. They each provide a portion of the total operational requirements necessary for an effective intelligence data dissemination architecture that supports the warfighter. IBS will migrate (combine) these legacy systems into a new system that has theater-focused dissemination architecture, with global connectivity, and uses a common information transfer language (standardized message formats). For the USN, the strategy for the implementation of IBS will be known as the Maritime Integrated Broadcast System (MIBS).

#### **2.8.6 RADIANT MERCURY**

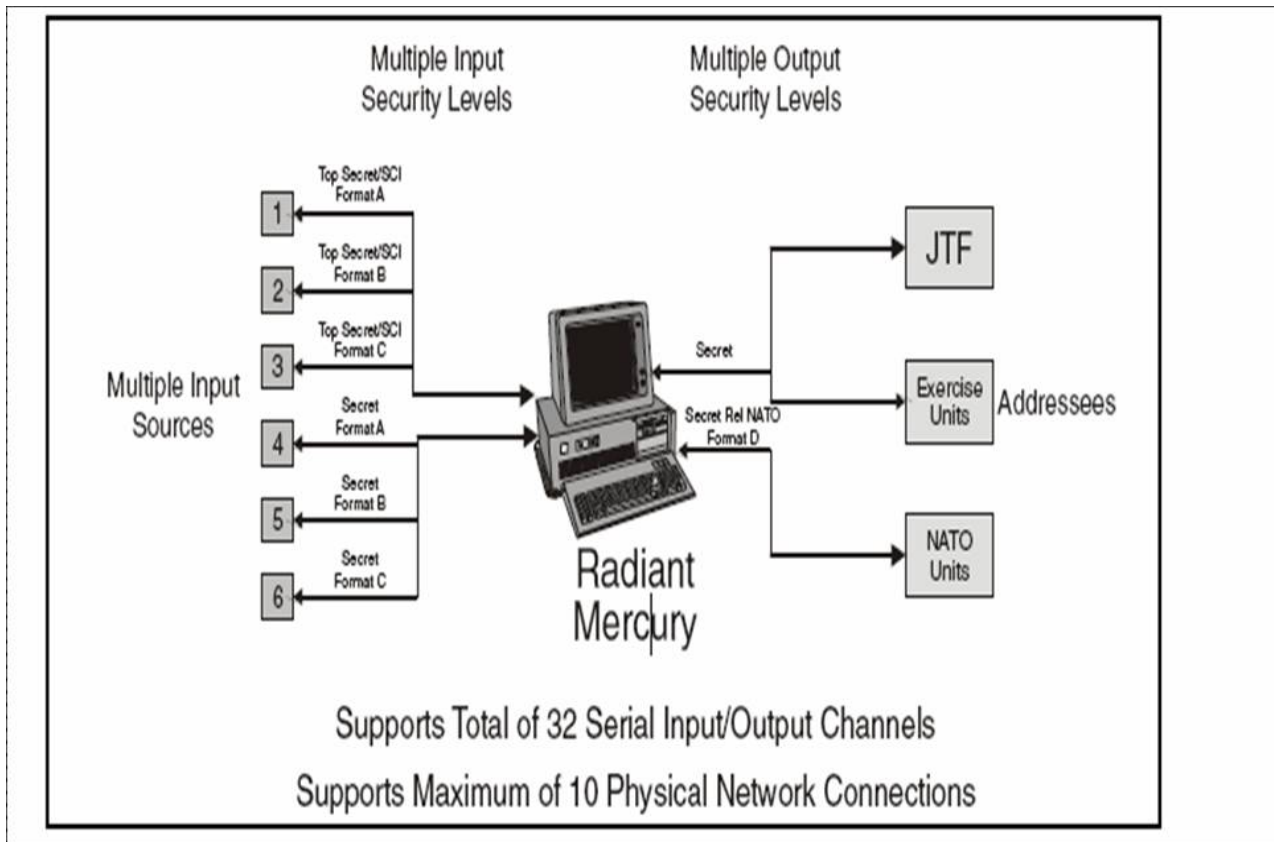
Radiant Mercury is a hardware and software application that automatically sanitizes and downgrades formatted data from SCI to GENSER. It is also used to sanitize data from U.S.-Only to Releasable for sharing with allied and coalition partners.

It only sanitizes formatted (OTG family, USMTF family, tabular, TDMIF, NITF, etc.) data. Message transliteration provides interoperability with other systems by allowing one format to come in and multiple different formats with the same data to go out (see Figure 2-16). The headers of NITF imagery files are formatted extensively, and Radiant Mercury is able to perform all of its capabilities on the header. Radiant Mercury cannot examine the image itself, so classified objects in the image pixels will pass through a Radiant Mercury screening untouched.

Radiant Mercury capabilities include:

1. Automating sanitization and guarding from higher to lower classifications
2. Downgrading to lower classification levels
3. Providing message format transliteration
4. Facilitating releasability to allies
5. Providing communications port guard (low to high)
6. Providing mechanism for data field integrity
7. Providing mechanism for selected data field checking
8. Providing a complete audit record
9. Supporting post event reconstruction

10. Providing dirty word searches on full text or specific fields.



**Figure 2-16**  
**Radiant Mercury**

### 2.8.7 SENSITIVE COMPARTMENTED INFORMATION NETWORKS

SCI networks (formerly SCI ADNS) provide multimedia delivery of tactical, administrative and intelligence information to ships at sea and provide ships access to shore cryptologic and intelligence resources. SCI networks are based on the integration of COTS/GOTS protocols, processors, and routers and provide network services such as secure e-mail, chat, websites, and file transfer.

The implementation of SCI networks will enable existing communications/network programs to migrate away from stove piped IXS protocols with their associated communications paths toward a single network with voice, video, and data transmission based on the TCP/IP protocol.

Depending on individual ship configuration, SCI networks use DSCS SHF, CWSP, UHF DAMA, EHF LDR/MDR, and Inmarsat-B HSD RF satellite connectivity through a single ADNS point of entry. Since the ADNS network operates at the GENSER SECRET level, SCI data is in-line encrypted to allow transport over the ADNS backbone using Motorola network encryption system (NES) devices. NES is capable of providing data confidentiality and integrity and peer identification and authentication, as well as mandatory/discretionary access control services. IP tunneling via the SIPRNET is used by SCI networks to reduce stovepipe connectivity, simplifies NES and network administration, and provides for secure alternate routing via standard ADNS connectivity.

Compartmented traffic, other than SI, is routed by SCI-ADNS to BORDERGUARD equipment and a separate computer workstation in SSES for use by appropriately cleared personnel.

#### **2.8.8 JOINT WORLDWIDE INTELLIGENCE COMMUNICATIONS SYSTEM (JWICS)**

The JWICS is operated by the Defense Intelligence Agency (DIA) as a secure global network designed to meet the requirements for TS/SCI multimedia intelligence communications worldwide. It provides users an SCI-level high-speed multimedia network using high-capacity communications to handle data, voice, imagery, and graphics. Secure e-mail, chat rooms, point-to-point and multipoint VTCs, broadcast of the DIN, and website access are the primary uses of JWICS by afloat users. The system also provides network services for collaborative electronic publishing, the electronic distribution of finished intelligence, and tools to accommodate the transfer of reference imagery, maps, and geodetic materials, as well as other high-end graphics products.



## CHAPTER 3

### MESSAGE PROCESSING PROCEDURES

#### 3.1 INCOMING MESSAGE HANDLING

##### 3.1.1 GENERAL

The term "incoming message" refers to all messages received by a telecommunications facility addressed to the parent command or subscriber, or accepted for relay by the telecommunications facility. Procedures for preparing/handling messages are contained in Annex D of NTP 3. Other procedures for unique systems and LANs should be documented in local SOPs.

##### 3.1.2 RECEPTION AND DUPLICATION CHECKING

Most of today's automated systems automatically log incoming messages and check for duplicates. Each NOVA system is configured with an auto delete function for every line with the exception of Yankee and Flash messages. The software examines each format line (F/L 2) and if it detects duplicate information from a previous message it automatically deletes the message without operator intervention.

##### 3.1.3 PRECEDENCE

Message drafters assign precedence to messages to indicate a desired writer to reader time. The criteria and speed of service (SOS) objectives for the four most commonly used precedence levels, Routines (Prosign R), Priority (Prosign P), Immediate (Prosign O), and Flash (Prosign Z) are defined in NTP 3.

There are two other important special purpose precedence categories (Refer to ACP 121 US-SUPP 1):

1. The CRITIC message contains information of vital importance and must be given the most rapid handling possible from origin to ultimate delivery to authorized recipients. Use the prosign W with this precedence when processing via Defense Special Security Communications System (DSSC) channels. Use the Flash (Z) prosign when processing the CRITIC message via general service (GENSER) channels. Messages are normally identified as CRITIC by placing "CRITIC" in the clear following prosign BT.
2. Emergency Command Precedence (ECP) is a time sensitive Command and Control Emergency Action Message (EAM) which

will be processed ahead of all other traffic. The prosign Y is designated for use on these messages to indicate Flash preemption capability. Only the National Command Authority (NCA) and certain designated commanders of unified and specified commands are authorized to use this precedence.

#### **3.1.4 INTERNAL DISTRIBUTION**

State of the art computer and communications equipment virtually eliminate the requirement for using paper in message distribution, for example:

1. Via GateGuard to an Electronic Mail (E-Mail) system on a LAN. Local communications SOP'S should document applicable procedures;
2. Dial-in using STU-III secure phone. Local communications SOP'S should document applicable procedures.

Internal reproduction and distribution procedures must never delay the dissemination of incoming urgent messages such as Emergency Action Messages (EAM'S). Individual telecommunications facility SOP'S will define the precedence levels of urgent messages. Communications personnel should be intimately familiar with these SOP'S. To expedite incoming information, the telecommunications facility will notify the appropriate action/cognizance office (or the command/staff duty officer after normal working hours) and note the time that this action occurred on the station log. The station log will also reflect the time-of-receipt, internal distribution and/or handling instructions and other additional information as appropriate, such as:

"(SDO/CDO/OOD) notified at (time)."

"Advance delivery to (SDO/CDO/OOD) at (time)."

"Portions received garbled; will service on request."

"Service action initiated."

"Corrected copy."

### **3.2 OUTGOING MESSAGE HANDLING**

#### **3.2.1 GENERAL**

The term "outgoing message" applies to all messages originated by a command.

The majority of outgoing messages will be handled by the telecommunications facility and delivered electronically. These procedures, however, are designed to cover most situations,

including the delivery of messages to a Quartermaster onboard ship for transmission. The focal point in processing outgoing messages is the main telecommunications facility which maintains the status of the message, and selects and directs the transmission medium for the message.

There are three types of Naval messages:

1. Operational messages directing or affecting the actual use of forces, ships, troops, and aircraft whether real or simulated; Those disseminating weather or other vital reports affecting the safety of life, ships, or forces; Those dealing with high command or nuclear strike coordination, tactical communications, combat intelligence, enemy reports, or information having a vital bearing on disposition, movement or employment of forces; Those which control communications, cryptography, deception and countermeasures, hydrographic and oceanographic information, and combat logistics matters.
2. Exercise messages are those relating to exercises conducted for fleet training and readiness, but are handled the same way as operational traffic. Messages are identified by "EXERCISE (name)" following message classification in the text. Text which reads "EMERGENCY STOP EXERCISE" and is sent via classified message and/or other authenticated means signals immediate termination of the exercise. Upon receipt, cease exercise conditions, cease relay of exercise messages and maintain present circuits until further notice. Code words may be used. The exercise directorate may direct resumption of the exercise by classified and/or other authenticated means.
3. Administrative messages are those covering matters which are neither operational nor exercise. The highest precedence may be assigned is Priority, except those messages reporting death, serious illness or injury which may be assigned IMMEDIATE precedence. The capacity of most afloat commands to receive the aggregate of operational and administrative traffic is limited. Therefore, administrative messages which include afloat commands shall be kept to a minimum.

### **3.2.2 MESSAGE RELEASE AUTHORITY**

All commands must adopt a message release policy that ensures that all messages delivered to the telecommunications facility have been properly released. Telecommunications facilities no longer verify release authority in the automated message processing environment. Release authority is an administrative function that must be exercised by the command entering messages into the communications system. To effectively control message release, commands should promulgate release authority lists

within their organizations via official correspondence, i.e., letters or notices.

A number of automated systems, such as the GCCS, Tactical Support Center (TSC) and other remote afloat and ashore terminals, are capable of automatically generating and releasing messages. Such messages can either be interfaced directly to a communications central processor such as a Nova for onward transmission or entered directly into communications channels. In such cases, the control of release authority is an administrative function of the command controlling the message traffic at the generating computer and there is no requirement for personnel at the servicing telecommunications facility to validate release or authorization.

Special situations the releasing authority must consider are as follows:

1. Minimize criteria is the originators responsibility. See NTP 3 for complete instructions on Minimize. Naval messages originated in or destined for an area under minimize will contain as the last line of text the statement "Released By name and rank/grade". PROFORMA messages which provide data that will be electronically entered into an automated database do not require a "Released by" line at the end of the message text.
2. Commands served by a telecommunications facility with PCMT or GateGuard must incorporate procedures for assigning message date-time-groups (DTG's). This procedure should be designed to prevent using duplicate DTG'S on messages from the same originator.

### **3.2.3 MESSAGE COMPLETENESS AND ACCURACY**

The responsibility for message correctness (proper use of dual precedence, construction of references, correct PLA'S, addition of special handling designators) rests with the originator. Messages containing errors are returned to the originator for correction, with the following exceptions:

1. For shore commands the servicing telecommunications facility will correct messages of IMMEDIATE and higher precedence.
2. For fleet/mobile commands the servicing telecommunications facility will correct all messages.

The only authorized source for U.S. activity short titles and geographical locations is in the Distributed Plain Language Address Verification System (DPVS). DPVS is a Navy developed system which allows electronic dissemination of, and electronic access to, PLA information. DPVS is intended for use by message drafters and is not solely a telecommunications facility tool.

NATO/Allied message addresses are located in the ACP 117 series of publications. If the telecommunications facility does not hold these documents, the correct PLA(s) should be requested from the serving telecommunications facility.

If a PLA is not in DPVS, the first step in verifying validity of the PLA is to check with the intended recipient. If the recipient verifies that the PLA is valid, consult ACP 117 and apply side routing. In all other cases, outgoing messages shall contain routing indicator "RHMCSUU".

Drafters are accountable for incorrect PLAs and shall ensure local procedures are established to reduce transmission of incorrect PLAs. Telecommunications facilities will assist by assisting originators in procuring approved message preparation software.

Assigning local internal distribution for outgoing messages is the responsibility of the drafter. Message copies/diskettes will reflect this information per NTP 3.

#### **3.2.4 CIRCUIT SELECTION AND DELIVERY**

Communications personnel need current information on active circuits so they may make an informed decision on which circuit should be used to transmit individual messages. Status boards must be maintained to display, at a minimum, a listing of stations on each circuit, and the condition of each circuit and station.

For high precedence/operational messages, the most expeditious route for delivery to action addressees, consistent with circuit classification, must be the foremost consideration in circuit selection. Any method or circuit will be used to expedite delivery of FLASH messages to all addressees within security constraints. To direct further processing, mark the specific means and circuit for transmission on the message draft and place in proper format for transmission, converting numerals and symbols to words as required by the selected method of transmission.

Forces afloat, at or near advance bases or staging points, should use fixed circuits for traffic to rear areas rather than ship/shore circuits. If not at anchor in the harbor, such traffic may be delivered to shore stations via low power local ship/shore or harbor nets. When in port, traffic should be delivered via FSM, CUDIXS or Gateguard.

### 3.2.5 TRANSMISSION OF CLASSIFIED MESSAGES UNDER EMERGENCY CONDITIONS

When the Commanding Officer determines emergency action is mandatory to affect delivery, messages of any classification may be transmitted via the lowest level cryptographically secured circuit. Additionally, under emergency conditions, information of any classification except TOP SECRET may be transmitted over any circuit using procedures in ACP 121 and ACP 128. In such cases, the originating command shall include the following handling instruction after the classification: CLEAR TRANSEC OVERRIDE AUTH. Compromises or suspected compromises resulting from exercise of this authority shall be reported in accordance with SECNAV M-5510.36.

### 3.2.6 MESSAGE CANCELLATION

When an outgoing message contains enough erroneous information that the originator must cancel it, a new message must be generated that, at a minimum, bears the same addressees, SSIC, and subject line as the original message. The cancellation text will reference the original date-time-group. Service messages will never be used for message cancellation. The cancellation of messages is a drafter/releaser responsibility.

#### MESSAGE CANCELLATION EXAMPLE

##### ORIGINAL MESSAGE

```
O 011757Z JAN 07
FM COMNAVNETWARCOM NORFOLK VA//N31/00/N3/N32//
TO AIG ONE THREE SEVEN SIX ZERO
INFO USS DWIGHT D EISENHOWER
BT
C O N F I D E N T I A L //N02300//
MSGID/GENADMIN/COMNAVNETWARCOM//
SUBJ/MSG EXAMPLE (U)//
RMKS/THIS MSG IS CLASSIFIED FOR DEMONSTRATION PURPOSES ONLY.//
DECL/X1//
BT
```

##### CANCELLATION MESSAGE

```
O 021427Z JAN 07
FM COMNAVNETWARCOM NORFOLK VA//N31/00/N3/N32//
TO AIG ONE THREE SEVEN SIX ZERO
USS DWIGHT D EISENHOWER
BT
UNCLAS //N02300//
MSGID/GENADMIN/COMNAVNETWARCOM //
SUBJ/MSG EXAMPLE//
```

REF/A/GENADMIN/COMNAVNETWARCOM/011757ZJAN00//  
 RMKS/CANCEL REF A//  
 BT

### 3.2.7 TRANSMISSION OF U.S. CLASSIFIED TRAFFIC TO ALLIED NATIONS

U.S. classified traffic specifically addressed to a friendly foreign nation or international pact organization and containing proper releasing per ACP 121 US SUPP-1, and OPNAVINST C5510.101 series, Security Manual for NATO, may be transmitted via the communications network for the foreign addressee provided the circuit is cleared for that particular message classification.

### 3.2.8 TRANSMISSION RELEASE CODE (TRC)

Transmission release code (TRC) facilitates automatic transfer of message traffic into Allied telecommunications networks. The TRC indicates to transfer stations that a message has been authorized for transmission to non-U.S. destinations or through non-U.S. circuits. TRC'S are not used on messages between U.S. activities transmitted entirely via U.S. telecommunications networks.

The TRC (not used in modified ACP 126 procedures) is a two-letter element located in ACP 128 format lines (F/L) two and four in conjunction with the security redundancy characters. Derivation of a TRC is based upon the second letter of the routing indicator of the foreign destinations. TRC assignments are as follows:

<u>COUNTRY</u>	<u>DESIGNATOR</u>
Australia	A
British Commonwealth (less Canada, Australia, New Zealand)	B
Canada	C
United States	U
NATO Countries (includes all member nations except the British Commonwealth and Canada)	X
New Zealand	Z

When two TRC'S are required on a message, they will be in alphabetical order. Only two TRC'S can be placed on one message for transmission. If, by composition of its addressees, a

message requires more than two TRCs, it must be transmitted twice; once with the first two TRC'S assigned, and a second time with the third and fourth assigned TRC'S. When using two TRCs, they must be in alphabetical order (i.e., AB, BC, CX, etc).

**EXAMPLE:**

CONFIDENTIAL MESSAGE TO AUSTRALIA AND A NATO COUNTRY  
F/L 2 P TTCZYUW RUFLABC0136 2131253-CCAX--RAXXX RXXXX.  
F/L 4 ZNY CCCAX

SECRET MESSAGE TO CANADA  
F/L 2 P TTSZYUW RUFLABC0136 2131253-SSCC--RCXXX.  
F/L 4 ZNY SSSCC

**3.2.9 SPECIAL HANDLING DESIGNATION (SHD)**

SHD'S were developed by Allied Nations and Regional Defense Organizations to mark messages for special handling between and within International Networks. Additional information on message drafting which requires SHD'S is found in NTP 3.

The SHD is represented by a letter of the alphabet, repeated five times, following the security redundancy on format line four. It is separated from the security redundancy by an oblique (/).

**EXAMPLE**

TOP SECRET SPECAT SIOP-ESI  
F/L 4 ZNY TTTTT/AAAAA

Messages that contain an SHD are controlled during electrical transmission process through a system of class marking the communications channels over which the messages can pass. The class marking inhibits the delivery of messages which contain a SHD to an authorized communications channel by means of a comparative validation check of the SHD shown in the message with the designators authorized for the communications channel.

SHD'S can be divided into three separate categories:

(1) AAAAA (SPECAT SIOP-ESI) and BBBBB (SPECAT other than SIOP-ESI) used only on US traffic; **(SCI networks only)**

(2) FFFFF (US-UK EYES ONLY) used on US originated, classified messages, addressed to activities of the United Kingdom (UK);

(3) LLLLL (ATOMAL), PPPPP (EXCLUSIVE) and YYYYY (CRYPTOSEcurity) used on US originated, classified messages addressed to NATO activities and/or NATO member nations.



### 3.3 SERVICE ACTION

#### 3.3.1 GENERAL

Service messages are short, concise messages between communication personnel. Such messages have the force of official communications and will be accorded prompt attention. Request for information will be kept to a minimum consistent with reliable communications to avoid overloading circuits and to protect security.

Communications officers may delegate release authority for service messages down to the communications watch supervisor. If action cannot be completed within reasonable time, the station originating the service will be so notified. Prosigns and operating signals will be used to the maximum extent to obtain and provide corrections or repetitions. Service messages are normally assigned a precedence the same as the message being serviced. Communication officers and communication watch officers are authorized to apply the NATO markings to service messages to NATO commands or activities when they are authorized NATO commands.

Service messages are addressed by the telecommunications facility to the serving Nova. If this site is unable to answer the request, it will service the originating station routing indicator (OSRI) of the message involved. All services will be retained until required action is complete. Information obtained via service action will be appended to the applicable message file copy of the serviced message. This may be done by attaching copies of the service(s) to the file copy or marking the date-time-group or OSRI SSN TOF of the service(s) on the file copy. The service message will also be filed separately as an incoming message.

Service messages will not be used to cancel official messages.

#### 3.3.2 OPERATING SIGNALS (OPSIG)

Operating signals, commonly referred to as "Q" and "Z" signals, are found in ACP 131 and its supplement, and provide a concise unclassified code designed for use by communications personnel to exchange information related to establishing communications or message handling. These signals provide no security and, therefore, must be regarded as plain language. "Z" signals are designed for use on military circuits. "Q" signals are used in non-military communications or whenever no suitable "Z" signal exists for military communications.

Operating signals should normally not be used in radiotelephone procedures, but when it is necessary, OPSIG'S are transmitted by

the phonetic equivalent.

Meanings for "Q" and "Z" signals may be amplified or completed with the addition of appropriate call signs, date-time-groups, etc. Plain language is prohibited except when no other method is available to complete the meaning.

When desired, an OPSIG may be given an interrogative sense by inserting the prosign INT before the appropriate "Q" or "Z" signal.

### **3.3.3 PROSIGNS AND PASSWORDS**

Prosigns listed in ACP'S 124, 126 and 127 are one or more letters, characters or combinations thereof. They are used to convey certain frequently used orders, instructions, requests or information relating to communications in a condensed standard form. Prowords are the spoken equivalents of prosigns for use in radiotelephone procedures.

Under no circumstances will operating personnel substitute prosigns or prowords for the textual component of a message received for transmission without the consent of the originator.

### **3.3.4 TRACER ACTION**

Tracer action is the process by which an investigation is conducted to determine the reason for an inordinate delay or non-delivery of a message. Proper tracer procedures are outlined in ACP 128.

### **3.3.5 MESSAGE CORRECTIONS AND CANCELLATIONS**

When an originating or relay station detects an error in a transmission, that station must send a correction by using a concise service or else ZDG/ZEL procedures. The OPSIG ZDS will not be used. The precedence of any corrective action will be equal to or higher than the original transmission. The receiving station is responsible for inserting all corrections indicated prior to distributing or filing the message.

The preferred method for Navy activities is to use a concise service, which is a brief message highlighting the incorrect portion of the original transmission. Voluntary corrections will reference the original date-time-group and be classified according to the actual classification of the corrected information. Corrections are preceded by the prosign "C" or proword "CORRECTION" and any required identifying data. An example follows:

ORIGINAL MESSAGE

PTTCZYUW RULSWCA1234 0311315-CCCC--RHMCSUU.  
 ZNY CCCCC  
 P 311300Z JAN 07 ZYB  
 FM COMNAVNETWARCOM NORFOLK VA//N31/N3//  
 TO AIG ONE THREE SEVEN SIX ZERO  
 BT  
 C O N F I D E N T I A L //N02300//  
 MSGID/GENADMIN/COMNAVNETWARCOM//  
 SUBJ/SERVICE PROCEDURES (U)//  
 RMKS/1. (C) THIS MSG IS CLASSIFIED FOR OPERATIONAL  
 PURPOSES ONLY.  
 DECL/X1//  
 BT  
 #1234

CORRECTION SERVICE MESSAGE

PTTUZYVW RULSWCA1235 0311405-UUUU--RHMCSUU.  
 ZNR UUUUU  
 P 311405Z JAN 07 ZYB  
 FM COMNAVNETWARCOM NORFOLK VA  
 TO AIG ONE THREE SEVEN SIX ZERO  
 BT  
 UNCLAS SVC //N00000//  
 C COMNAVNETWARCOM NORFOLK VA 311300Z JAN 07  
 LINE 1 CHANGE WA FOR TO READ TRAINING.  
 BT  
 #1235

When a message is garbled or incomplete, send a request for a retransmission (INT ZDK) using a service message as listed in the service section of ACP 128.

If it is imperative that a message, such as one with high precedence, be forwarded without correction, the operating signal ZDG (accuracy of following message doubtful) will be included. When a corrected copy of such a message is required, only the operating signal ZEL (meaning: this message is a correction) will be used for follow-up transmissions.

**3.4 MESSAGES REQUIRING SPECIAL HANDLING****3.4.1 GENERAL**

On occasion, messages between commanders must receive special handling and distribution in addition to that afforded by the assigned security classification. To identify such messages, message drafters/releasers are responsible for determining the need for and apply special handling designations or delivery instructions, and to correctly place them within the message text.

### **3.4.2 SPECIAL CATEGORY (SPECAT) MESSAGES GENERAL**

SPECAT is a designation applied to classified messages identified with a specific project or subject requiring special handling procedures supplemental to those required by the security classification. The special handling procedures are designed to prevent handling and viewing by other than properly cleared and authorized personnel.

Clearances for personnel handling and processing SPECAT less SIOP-ESI messages will meet the criteria promulgated in SECNAV M-5510.36 (Department of the Navy Information Security Program Regulation). Within communications channels, personnel, including maintenance personnel, who may require access to or operate terminals, communications equipment, or automatic data processing equipment which processes SPECAT messages, will be designated in writing by the Commanding Officer of the communications facility involved and briefed on the sensitivity of the information in SPECAT traffic.

SPECAT messages may be transmitted on-line without prior encryption if the entire circuit path is cleared for the security classification of the message involved.

On-line transmission of SPECAT, less SIOP-ESI, with a classification up to and including TOP SECRET, to any State Department addressee or DOD field activity serviced by the Diplomatic Telecommunications Service (DTS) is authorized and shall be effected by the use of the current State Department special purpose on-line routing indicator. On-line transmission of SPECAT SIOP-ESI through the DTS is prohibited.

SPECAT message originators will insert the "SPECAT" designator immediately following the message classification and preceding the project or subject name. This will facilitate the proper handling and ensure minimum dissemination required for these messages during transmission and processing. See NTP 3 for complete instructions for drafting SPECAT messages.

If necessary, a copy of a SPECAT may be retained on the communication officer's special file or by the Top Secret Control Officer (TSCO). Under no circumstances will a copy of a SPECAT message be retained in the crypto center files or on the on-line monitor reels. Worksheets, excess copies, and carbon used in preparing and/or processing these messages will be immediately destroyed by burning or shredding.

### **3.4.3 SPECIAL CATEGORY (SPECAT) SIOP-ESI**

Special Category (SPECAT) Single Integrated Operational Plan - Extremely Sensitive Information (SIOP-ESI) messages require stringent controls over reproduction, dissemination, transmission, access and accountability and is not permitted on

Genser networks only networks certified SCI. SIOP-ESI messages shall be classified TOP SECRET only and must contain the SPECAT caveat. Commands that are required to process SIOP-ESI messages must certify that the provisions of OPNAVINST S5511.35, Policy for Safeguarding SIOP, have been met.

SIOP-ESI messages will be logged and disseminated to the subscriber's SIOP Control Officer only. These messages will be placed in a SIOP-ESI file with fillers in appropriate files. The SIOP control officer will regulate further distribution and account for these messages per OPNAVINST S5511.35.

**Clearance and Access.** Only those communications personnel involved in the actual processing of SIOP-ESI messages should be processed for clearance or granted access to SIOP-ESI. The number of personnel requiring SIOP-ESI clearance and access is a command decision commensurate with actual processing, training, and replacement requirements. All personnel working in or having access to areas where SIOP-ESI material is processed need not have SIOP-ESI clearance. However, control procedures must be established to ensure against exposure of the material. Should inadvertent disclosure of SIOP-ESI information to non-authorized personnel occur, debriefing is required, in accordance with guidance contained in OPNAVINST S5511.35. Procedures for requesting clearance for and granting access to SIOP-ESI information are specified in OPNAVINST S5511.35 series.

#### **3.4.4 SPECIAL CATEGORY (SPECAT) EXCLUSIVE FOR**

The SPECAT EXCLUSIVE FOR (SEF) message was established for those rare classified matters requiring the highest degree of privacy between individuals as opposed to command or offices. Within the Navy, SEF is reserved for use by Flag and General Officers, or officers in command status. SEF messages are not intended for use in operational matters, but rather, for transmission of certain high level policy or politically sensitive matters limited to the eyes of the named recipient only. Initial distribution is limited to the person whose name, title, or designation appears on the message. These messages are logged in accordance with the classification, but are maintained in the cryptocenter file with fillers in appropriate files.

SEF will not be used for matters which require extensive staff support for either the originator or the recipient. SEF will not be used in reply to a SEF message unless the contents of the reply so dictate. SEF messages will normally not be cited as references and SEF messages shall not be readdressed.

#### **3.4.5 TIGHT CONTROL (TICON)**

OPNAVINST C3490.1 contains detailed procedures prescribed for TICON messages.

### 3.4.6 EMERGENCY ACTION MESSAGES

Fast reaction communications are procedures established to ensure timely flow of information from the National Command Authorities (NCA) to the lowest level of command, and from the lowest level of command to the NCA, when the information to be passed meets the criteria for such direct communication. These are FLASH precedence messages and take priority over all other FLASH traffic except certain Emergency Action Messages (EAMs). The ultimate goal is receipt of this critical information by all addressees within the prescribed time criteria.

Evaluation of Fast Reaction Communications exercises indicates a continuing need for command interest in and familiarity with fast reaction communications procedures. Commanding officers shall ensure appropriate operating personnel are thoroughly familiar with the intent and procedures for establishing fast reaction communications. Internal procedures must be devised to assure efficient and timely response to fast reaction situations, real or exercise.

It has been determined that fast reaction exercises are the best means to train for actual situations. Should a need arise, there will be no time to "research the problem." The keynote to fast reaction remains in the preparation and thorough knowledge of procedures on the part of all concerned. All levels of command, mobile or shore-based, are subject to involvement in Fast Reaction Exercises outlined herein.

### 3.4.7 WHITE PINNACLE (EA CELL) MESSAGE INJECTS

Theater CDR will direct commands and units, by FLASH message, to initiate a WHITE PINNACLE report to the JCS/NMCC.

#### Example:

```
Z 030303Z DEC 07
FM CDR USJFCOM NORFOLK VA
TO USS XXXXXX
INFO ADDEE: INFO IEMATS NMCC
UNCLAS //N02740//
MSGID/GENADMIN/CDR USJFCOM//
SUBJ/EXERCISE WHITE PINNACLE//
RMKS/1. UPON RECEIPT OF THIS MESSAGE, ORIGINATE
EXERCISE WHITE PINNACLE (OPREP-3) TO JCS/NMCC.
EXERCISE WHITE PINNACLE//
```

Either voice or record communications may be used to report WHITE PINNACLE messages to NMCC. Voice circuits are preferred; however, a choice of a communications system is a matter of judgment on reliability and timeliness. Upon receipt of the order message, the command and/or unit designated will originate and transmit a WHITE PINNACLE report to JCS/NMCC as follows:

#### **3.4.8 LIMITED DISTRIBUTION (LIMDIS)**

LIMDIS messages are associated with special projects, cover names, or specific subjects such as urinalysis screening results that require limited internal screening and distribution. The intent and meaning of LIMDIS is to limit distribution of copies or electronic delivery of such messages to those specifically authorized to have access to the information. The commanding officer, not the communications officer, determines distribution of LIMDIS messages. When a LIMDIS message relating to a special project, cover name, or other criteria is drafted, it is the originator's responsibility to ascertain that all addressees are authorized recipients of that type of traffic. Commands will furnish to their serving NTCC a list of authorized local recipients of LIMDIS messages. If a particular LIMDIS subject does not appear on this list, the NTCC will determine the action or cognizant office or officer on the basis of the message's content and provide one copy to him/her only until he/she directs any additional dissemination.

#### **3.4.9 AMERICAN RED CROSS (AMCROSS)**

In order to ensure rapid delivery, up to IMMEDIATE precedence may be assigned to AMCROSS messages concerning death or serious illness. Additionally, EFTO markings should not be applied to AMCROSS traffic, because such action incurs excessive delays and results in needless manual handling.

AMCROSS messages contain information very personal to the intended recipient. Therefore, communications personnel will not discuss the contents of such a message with anyone and will limit the message distribution to the executive officer or an appointed alternate only. Local command policy will dictate filing procedures for AMCROSS messages.

#### **3.4.10 TOP SECRET**

TOP SECRET messages are not in themselves SPECAT messages. Top Secret is a standard security classification as defined by existing Department of Defense and service instructions. The term SPECAT will not be used on messages classified TOP SECRET, except when a TOP SECRET message is concerned with a project or subject which meets the criteria specified for SPECAT messages. For TOP SECRET message traffic addressed to the parent command of the telecommunications facility, log the message in accordance with paragraph 3.6.4. Give the only copy to the TOP SECRET control officer for entry into the command's controlled distribution system.

For TOP SECRET messages received by an afloat command but not addressed to that command, only the text will be removed from the broadcast rolls and ticklers entered in the broadcast files. The message text will be destroyed immediately by authorized methods and destruction certified by the two witnessing officials placing

their initials on the broadcast monitor roll and next to the appropriate broadcast serial numbers on the check-off sheet. Check-off sheets and file fillers are exempted from the regulation requiring that certificates of destruction be retained for two years and will instead be destroyed with the broadcast files.

TOP SECRET message traffic handled by communications stations (for relay or broadcast delivery only) need not be controlled and accounted for as described in DODINST 5200.1 series and SECNAV M-5510.36 providing all copies, less monitor roll, are destroyed immediately after having served their purpose. Monitor rolls will be marked TOP SECRET and afforded TOP SECRET security and storage. After retention for the mandatory period, they will be destroyed per SECNAV M-5510.36.

The responsibilities of a naval communications facility for over-the-counter delivery of TOP SECRET traffic are as follows:

1. Upon receipt of a TOP SECRET message addressed to a customer, the telecommunications facility will log the message in accordance with paragraph 3.6.4.
2. The telecommunications facility will notify the customer of receipt of the TOP SECRET message. The message will be delivered only to a courier specifically authorized in writing by his/her command for receipt of TOP SECRET traffic. The courier must present a valid military/government identification card for communications personnel to verify against the guard command's TOP SECRET courier list.
3. TOP SECRET, Special Category (SPECAT), and Tight Control (TICON) messages are authorized for diskette or paper copy delivery. The customer's designated command courier will be provided the message(s) on a separate diskette(s) or in a separate folder (if delivery is accomplished by paper copy) with a disclosure sheet filled out per SECNAV M-5510.36.

#### **3.4.11 PERSONAL FOR**

PERSONAL FOR messages are those classified and unclassified messages marked "PERSONAL FOR" a person by name or title, and are treated as a personal message. The use of PERSONAL FOR messages is reserved for officers of flag rank and officers in a command status. This special delivery instruction is intended to insure greater privacy than ordinary messages and to convey information on a personal basis. Distribution is made solely to the designated recipient. Additional distribution may be made as directed by the recipient.

PERSONAL FOR messages are handled by regularly assigned communications personnel who possess a security clearance



commensurate with the classification of the particular message. Do not use any special procedure to account for, log, or destroy PERSONAL FOR messages, i.e., attach a disclosure sheet, etc., except as specifically required by the classification applied to the individual message. Transmit PERSONAL FOR messages per the classification of the message.

### 3.5 MESSAGE FORMATS

#### 3.5.1 GENERAL

Messages transiting the Defense Information Infrastructure (DIS), of which the Naval Computer and Telecommunications System (NCTS) is an integral part, vary in format. Depending upon the present level of processing and ultimate destination of the message, the format will be ACP 126, modified ACP 126, ACP 128 or ACP 127. Message preparation procedures are found in NTP 3.

The major differences between these formats appear in the first three format lines (F/L) of the message heading. All four formats are similar with only minor variations from F/L 4 through F/L 16.

#### 3.5.2 ORIGINATING STATION ROUTING INDICATOR (OSRI)

Ships will derive an originating station routing indicator (OSRI) by using the first four letters of the routing indicator of the Fleet NARC assigned to the servicing NCTAMS/NAVCOMTELSTA system to which they will transmit, suffixed by FRI assigned to the fleet/mobile unit. The OSRI will always consist of seven letters and will be located in fields 10-16 of F/L 2. For example, if USS KENNEDY accessed CUDIXS with NCTAMS LANT the OSRI would be RHBAJFK, "RHBA" being NCTAMS LANT'S Fleet NARC and "JFK" being the three letters of KENNEDY'S FRI designator.

The following procedures apply when a command, unit, DET, etc., embark on a fleet unit under conditions that require assignment of a temporary routing indicator:

(1) The embarking command will request assignment of a FRI designator from the MASTER UPDATE AUTHORITY Honolulu, HI. To insure timely promulgation and data base up-dates, the request for routing indicator assignment should be forwarded by message five days in advance of activation. Note that every mobile PLA requires an FRI. The message will contain the following information (repeat para a as needed):

SUBJ/REQUEST A TEMPORARY/PERMANENT FLEET ROUTING INDICATOR  
(FRI)//  
RMKS/1. REQUEST AN FRI FOR THE FOLLOWING PLAIN LANGUAGE ADDRESS  
(PLA):  
(A) PLA:

(1) OFFICIAL COMMAND/ACTIVITY NAME BY LONG TITLE TO INCLUDE GEOGRAPHIC LOCATION IF APPLICABLE.

(2) DATE-TIME-GROUP (DTG) FOR FRI ACTIVATION.

(3) DTG FOR DEACTIVATION OF TEMPORARY FRI.

(4) REASON FOR FRI ESTABLISHMENT.

(5) POINT OF CONTACT (POC) WITH PHONE NUMBER/E-MAIL ADDRESS.

(2) Once the PLA is approved and FRI assigned, fleet/mobile units must submit an ESTABLISHMENT COMMSHIFT to promulgate the new PLA. (Refer to NTP 4 Supp-2)

(3) It is the responsibility of the requesting unit to disestablish both temporary and permanent PLA's and corresponding FRI'S by submitting DISESTABLISHMENT COMMSHIFT'S. (Refer to NTP 4 Supp-2)

**3.5.3 STATION SERIAL NUMBER (SSN)**

The originating station serial number (SSN), located in fields 17-20 of F/L 2 and also in F/L 15, will consist of four digits (0001-9999) and will be assigned sequentially. In combination with the OSRI, the SSN provides positive identification for each transmission. SSN "0000" will be used only in quality control test messages as stated in Paragraph 341, ACP 128. Duplicate SSN's will not be assigned within any five-day period.

**3.5.4 ROUTING**

Generally, US Navy mobile units are not required to maintain ACP 117 and its supplements. Activities route regular traffic to MCS using routing indicator "RHMCSUU". Service action messages are sent to the PLA DUSC LANT, DUSC PAC, DUSC EURCENT.

<u>COMMON MESSAGE FORMAT LINES (F/L)</u>	
F/L	Message Components
4	Security warning, security classification code, transmission release code (TRC), special handling designator(s) (SHD) transmission instructions
5	Precedence, originator's date-time-group, message instructions
6	Message originator (FM)
7	Action addressees (TO)
8	Information addressees (INFO)
9	Exempt addressees (XMT)
11	Prosign BT
12	Message text will be arranged in the following order (as applicable):

	a. Security classification
	b. Special handling designations, e.g., SPECAT, US-UK EYES ONLY, etc.
	c. Releasability statement
	d. Special delivery instructions, e.g., PERSONAL FOR
	e. Standard subject identifier codes (SSIC), subject indicator code (SIC), delivery distribution indicator (DDI)
	f. Exercise name
	g. Subject line (SUBJ)
	h. References
	i. Thought or idea
	NOTE: Items a., g., and i. are mandatory in narrative messages, remainder as needed.
13	Prosign BT
14	Confirmation
15	End-of-message (EOM) validation consisting of number sign (#) and 4-digit station serial number (SSN)
16	EOM functions, 2CR, 8LF, 4Ns, 12 LTRs, In ACP 126 format, also use prosigns "K" or "AR"

**Figure 3-1. Common Message Format Lines**

### 3.5.5 ACP 128

ACP 128 format shall be used by personnel of all nations and agencies in the preparation, transmission, and handling of record communications exchanged among communications facilities served directly by the ALLIED TELECOMMUNICATIONS RECORD SYSTEM (ALTERS).

The ALTERS is a world-wide common user telecommunications system which provides for the transmission of narrative traffic on a store-and-forward basis. The world-wide system is composed of national/regional defense force organization telecommunications systems interconnected for the exchange of information of mutual interest. The objective of ALTERS is to provide a reliable, secure and efficient common user communications system which incorporates error detection techniques. ALTERS does interface with DMS. For more amplifying information refer to ACP 128 (A) dated June 2005.

Messages will be prepared in one of three formats for transmission via the ALTERS; Plaindress, Abbreviated plaindress or Codress.

#### **PLAINDRESS**

```

2 RTTUZHSW RUEBABA1234 1081400-UUUU--RUKKLAA.
4 ZNR UUUUU
5 R 181230Z JUL 07
6 FM AFSC ANDREWS AFB MD
7 TO ELMENDORF AFB ALASKA

```

11BT  
 12 UNCLAS (TEXT)  
 13 BT  
 15 #1234  
 16 (2CR) (8LF) NNNN (12LTRS)

**ABBREVIATED PLAINDRESS**

2 PTTCZHSW RUCLDBA0123 1081400-CCCC--RUHHLFA..  
 4 ZNY CCCCC  
 11 BT  
 12 C O N F I D E N T I A L (TEXT)  
 13 BT  
 15 #0123  
 16 (2CR 8LF) NNNN

**CODRESS**

2 RTTUZHSW RUEOLGA0025 1081400-UUUU--RUCIABA.  
 4 ZNR UUUUU  
 5 R 181320Z APR 07  
 10 GR55  
 11 BT  
 12 XXXXX XXXXX XXXXX XXXXX (TEXT)  
 13 BT  
 15 #0025  
 16 (2CR 8LF) NNNN

**3.5.6 MODIFIED ACP 126**

Modified ACP 126 format is designed to allow Navy users of the Defense Information System (DIS) to send traffic without assigning routing indicators in F/L 7 and 8. This format also removes the requirement to maintain routing doctrines (ACP 117 series publications) by the majority of Navy activities.

MESSAGE IN MODIFIED ACP 126 FORMAT

<u>F/L</u>	<u>MESSAGE COMPONENT</u>
1	Use ACP 128 preamble (VZCZC), circuit identification, channel sequence number.
2	Same as in ACP 128 except use the world-wide MCS routing indicator RHMCSUU.
4	In this format, transmission release codes (TRCs) are assigned by MCS Special Handling Designators (SHD) are the responsibility of the drafter.

F/L MESSAGE

1 VZCZCABC123

2 RTTCZYUW RULSWCA5678 0031235-CCCC--  
RHMCSUU.

4 ZNY CCCCC  
5 R 031234Z JAN 00  
6 FM COMNAVNETWARCOM NORFOLK VA//N61/N6//  
7 TO COMUSNAVEUR LONDON UK//N6//  
MODUK

8 INFO USS DWIGHT D EISENHOWER

11 BT

12 C O N F I D E N T I A L //N02300//  
MSGID/GENADMIN/COMNAVNETOPSCOM//  
SUBJ/SAMPLE MESSAGE//  
RMKS/THIS IS A MODIFIED ACP 126 MESSAGE  
CLASSIFIED FOR TRAINING PURPOSES ONLY.  
DECL/X1//

13 BT  
15 #5678  
16 NNNN

### 3.5.7 ACP 127

ACP 127 format is used on NATO circuits. For US traffic, AUTODIN is responsible for format conversion.

<u>F/L</u>	<u>MESSAGE COMPONENT</u>
1	Transmission identification, including Start of Message" function.
2	Repeated precedence, routing indicators of stations responsible for delivery or refile.

To illustrate the transition from ACP 128 to ACP 127, the following depicts the converted version of the ACP 128 example into ACP 127 format:

#### MESSAGE IN ACP 127 FORMAT

F/L    MESSAGE

1        VZCZCHYA076  
2        RR RHDLCNE RBDWC  
3        DE RULSWCA5678 0031235  
4        ZNY CCCBB  
5        R 031234Z JAN 00  
6        FM COMNAVNETWARCOM NORFOLK VA//  
7        TO RHDLCNE/COMUSNAVEUR LONDON UK RBDWC/MODUK  
8        INFO RHBAIKE/USS DWIGHT D EISENHOWER  
11       BT

12       C O N F I D E N T I A L //N02300//  
MSGID/GENADMIN/COMNAVNETWARCOM//  
SUBJ/SAMPLE MESSAGE//  
RMKS/THIS, AN EXAMPLE OF A ACP 128 PLAINDRESS  
MESSAGE (CONVERTED TO ACP (127), IS CLASSIFIED

FOR TRAINING) PURPOSES ONLY.  
 DECL/X1//  
 13 BT  
 15 #5678  
 16 NNNN

When service action is required, always cite information from F/L 3 (OSRI, SSN and TOF).

### 3.5.8 ACP 126

For most teletypewriter point-to-point circuits, such as TASK FORCE ORESTES, the format employed is ACP 126. This format does not require any routing indicators.

<u>F/L</u>	<u>MESSAGE COMPONENT</u>
2	Station called who is responsible for delivery.
3	Station making transmission, station serial number.
16	Use of prosigns "K" or "AR" as EOM function.

#### MESSAGE IN ACP 126 FORMAT

F/L    MESSAGE  
 2        NUSA  
 3        DE NIKE 4321  
 4        ZNR UUUUU  
 5        R 041235Z JAN 00  
 6        FM USS DWIGHT D EISENHOWER  
 7        TO USS ENTERPRISE  
 11       BT  
 12       UNCLAS //NO2300//  
          MSGID/GENADMIN/USS EISENHOWER//  
          SUBJ/SAMPLE MESSAGE//  
          RMKS/THIS ILLUSTRATES ACP 126  
          FORMAT FOR POINT-TO-POINT TRAFFIC.//  
 13       BT  
 16       K

### 3.5.9 DEFENSE SPECIAL SECURITY COMMUNICATIONS SYSTEM (DSSCS)

General Service (GENSER) communications provide worldwide defense force telecommunications services for the exchange of information of mutual interest.

General Service (GENSER) systems, such as the Defense Message System (DMS) and the Automated Digital Information Network (AUTODIN), provide for delivery of record communications through the use of store-and-forward message systems, message switching systems, and dedicated circuitry. In the GENSER category alone, there are over 315 types of messages, not including NATO designations. All U.S. organizations and activities that utilize these communications must abide by Naval Telecommunication Publications (NTPs) and Allied Communications Publications (ACPs).

Defense Special Security Communications System (DSSCS) is the organization through which the Director, DIA, and the Military Department Intelligence Chiefs accomplish their responsibilities for the security, use, and the dissemination of Special Intelligence, to include both physical and electrical means. Officers assigned to the System are referred to as Special Security Officers (SSOs). The local senior SSO is that officer specifically designated by the Director, DIA, or the appropriate Military Department Intelligence Chief for the implementation of Communications Intelligence (COMINT) security and administrative instructions.

The system refers to the world-wide special purpose communications system for the processing and exchange of formatted signal and critical intelligence messages and other sensitive or privacy information referred to as Special Compartmented Information (SCI). The DSSCS community is also served by DMS, AUTODIN, Defense Message Dissemination System (DMDS), and Automated Digital Networking System (ADNS) plus community unique systems, such as NEWSDEALER. SCI is exchanged by the use of a unique message format. Defense Special Security Communications System (DSSCS) Operating Instruction 103 (DOI 103) provides the operating procedures and practices applicable to Special Security, Signal Intelligence (SIGINT), and other sensitive communications facilities processing Special Compartment Information (SCI) messages.

The primary difference between GENSER and DSSCS message formats are:

1. Different routing indicator structure.
2. The use of message format line four alpha (4a.)
3. Different Transmission Control Code (TCC) format and selection.

For the purposes of this document, a brief description is provided; however, full explanations are contained in DOI-103.

#### **3.5.9.1 DSSCS PLAIN LANGUAGE ADDRESSES AND ROUTING INDICATORS**

GENSER Routing Indicators begin with the letter "R" and are seven characters in length. DSSCS routing indicators begin with the letter "Y" and are normally six characters in length.

##### **Composition**

DSSCS routing indicators are assigned by the Director, National Security Agency from a block allocated by the Director, Defense Information Systems Agency. Assignment of a DSSCS routing indicator is based on the type of activity and on the provision the activity has a certified Plain Language Address (PLA) listed in the USSID 309, USSID 505, or the DIA Compartmented Address Book

DSSCS routing indicators normally consist of six letters. The letter "C" may be suffixed to any DSSCS routing indicator to designate delivery responsibility. It is used to designate a specific activity as over-the-counter (OTC) guard for an addressee who has no assigned routing indicators. When a message is routed to such an addressee, the letter "C" suffixed indicator followed by a slant sign must precede the pertinent addressee designation in the address portion of a multiple address message. Additional sources for OTC guard are the United States Signal Intelligence Directive 505 (USSID 505) and the DIA Compartmented Address Book.

#### **DSSCS Address Group**

Collective address groups shorten the message preparation time and the message length; thereby reducing the communication handling time. DSSCS Operating Instructions 101 (DOI 101) describes the purpose and assignment of these collective routing groups called DSSCS Address Groups (DAGs).

DAGs are prescribed for use in routing general messages and represent a specific group of addressed activities. Collective and single addresses/routing indicators can be used in the same message heading.

A DAG PLA is five characters in length and do not form a word. When using a DAG in the "TO" line, individual addressees that are a part of the predetermined list do not have to be placed in format line 7, however, their routing indicator must be placed in format line 2. An addressee cannot be removed from a DAG without the use of the prosign "LESS" preceding that plain language address of the addressee. If multiple addressees are to be excluded, "LESS" must precede each addressee. The following illustrates an example of the use of a DSSCS address group:

```
ZCZCNAA633
PTTMZYUW YEIDNA 0019 1941014-MNSH-YAIARI YAIDDL
YAIDHA YAIDNI YAIDNR YEKAH YEXRAD YHLADL YWHAIK
YSNAIH.
ZNY MMNSH
ZKZK PP XAA DE
P 130057Z JUL 07
FM USM-86
TO ABAXI
LESS USM-653
INFO CDRINSCOM
ZEM
C L A S S I F I C A T I O N
QQQQ
TEXT
#0019
```

NNNN



**Addressing Limitations**

A multiple address message is limited to a maximum of 500 PLAs/routing indicators and a maximum of 15 collective addresses/routing indicators.

**3.5.9.2 LEGACY ADDRESS DIRECTORY SERVICE (LADS)**

Legacy Address Directory Service (LADS) is a system designed to provide centralized dissemination of DSSCS routing information contained in DOI-101 (DSSCS Address Group - DAGs), DOI-102 (DSSCS PLAs), and GENSER routing information provided by DISA.

The LADS query tool is a JWICS based, web application that allows queries against the database from any web browser. Up-to-date routing information is readily available to the SCI community.

**DSSCS Message Format**

DSSCS message format consist of three parts: The HEADING, format lines 1 through 11; the TEXT, format lines 12, 12A and 12B; and the ENDING format lines 15A and 16. The order or relative position of the elements within each line may not be altered; however format lines 7, 8, 10, and 15 may be omitted, singly or collectively, if not needed for a particular message. All other format lines are required on messages except service messages, as explained in chapter 5 of the DOI-103.

**DSSCS Message Schematic**

Explanation of each line of a DSSCS format message is as follows:

Line 1 - Contains the Start of Message (SOM) indicator, Channel Designation and Sequence Number (CDSN).

Line 2 - Contains the following information in character position as indicated:

- (a) Position 1 - The precedence prosign of the message.
- (b) Position 2 and 3 - Language Media and Format (LMF).
- (c) Position 4 - Security - The Special Intelligence community prosign is "M".
- (d) Position 5 through 8 - Content Indicator Code/Communications Action Identifier - Consists of four alphabetical characters or three alphabetical characters and 1 numerical indicator character.
- (e) Position 9 - Separator - A space will be placed in this position.
- (f) Position 10 through 15 - Originator The routing indicator of the originating station will be placed in these positions.
- (g) Position 16 through Separator - A space will be placed in this position.
- (h) Position 17 through 20 - Station Serial Number - Consists of four numeric characters.
- (i) Position 21 through Separator - A space will be placed in this position.

(j) Position 22 through 24 - Date - The ordinal date on which the message was received from an originator by the communications center for transmission.

(k) Position 25 through 28 - File Time - The time (GMT) the message was received from an originator by the communications center for transmission.

(l) Position 29 - Security Sentinel - A hyphen (-) is used to indicate that the security and transmission control code.

(m) Position 30 Security - The Special Intelligence community prosign is "M".

(n) Position 31 through 33 - Transmission control code (TCC) - The TCC "NSH" indicates "No Special Handling". Other trigraphs are assigned to denote special handling requirements (reference DOI-103 paragraph 308).

(o) Position 34 and 35 - Start of Routing - Two consecutive hyphens preceding the first routing indicator.

(p) Position 36 through as required - Routing - Addressee routing indicators are listed immediately following the start of routing signal. A maximum of 4 routing indicators will be on the first line of format line 2, with a maximum of 9 routing indicators on each successive line are required. A maximum of 500 routing indicators can be listed in a single transmission. Routing indicators are separated by a space and are not required to be in alphabetical order.

(q) Position 37 - End-of-routing - A period (.) inserted in the position immediately following the last addressee's routing indicator.

Line 3 - Not used in DOI-103 format

Line 4 - Security warning operating signal ZNY followed by the Special Intelligence community prosign "MM" and the appropriate TCC.

Line 4A - Director Line - Elements necessary to accomplish switching of message traffic at communications centers equipped with an automated message distribution. The elements are:

- (a) Switching function "ZKZK" (followed by a space)
- (b) Repeated precedence prosign (followed by a space).
- (c) First DDI and succeeding DDI's (if required) followed by a space.
- (d) Switching function "DE"

Line 5 - Precedence Prosign, date-time-group followed by the abbreviated month and year, and message instructions in the form of operating signals. The operating signal "ZYH" will appear in this line on all CRITICs and messages assigned FLASH or IMMEDIATE precedence.

Line 6 - Prosign "FM" and the Plain Language Address (PLA) of the originator.

Line 7 - Prosign "TO" and the designation of the action addressee(s) in the form of the assigned station designator,

administrative title, or address group(s). Also contains "C" suffix routing indicators when applicable.

Line 8 Prosign "INFO" and the designation of the information addressee(s) in the form of the assigned station designator, administrative title, or address group(s).

Line 9 - Not used in DSSCS.

Line 10 - Group count prosign "GR" and the number of groups in the message text.

Line 11 - Start of Text (SOT) line containing the operating signal "ZEM"

Line 12 - Classification information line

Line 12A - "QQQQ" Special delimiter used to separate classification and special handling instructions from remainder of text.

Line 12B - Remainder of text

Line 13 and 14 - Not used in DSSCS

Line 15 - Prosign "C" and any necessary corrections.

Line 15A - End-of-message (EOM) validation number preceded by a number symbol.

Line 16 - EOM functions (2CR, 8LF, 4N's, 12 LTRS)

The following examples illustrate the proper sequence of elements in message preparation:

```

Line 1 - ZCZCHAC157
Line 2 - RTTMZYUW YEKSHA 0103 1232037-MNSH--YEKAAH YEKDQH.
Line 4 - ZNY MMNSH
Line 4A - ZKZK RR SOA DE
Line 5 - R 031950Z MAY 07
Line 6 - FM CNO
Line 7 - TO DIRNSA
Line 8 - INFOR JCS
Line 11 - ZEM
Line 12 - C L A S S I F I C A T I O N
Line 12A - QQQQ
Line 12B - TEXT
Line 15 - C: (CORRECTION IF NEEDED)
Line 16 - #0103

```

Line 16 - NNNN

### **3.5.9.3 CLASSIFICATION OF MESSAGES (TRANSMISSION CONTROL CODES)**

The primary classification of each message is contained in message format line twelve, beginning with the basic classification, followed by caveats, codewords, and/or special handling instructions.

Transmission Control Codes (TCC) are a three letter code which is placed in both format lines two and four, and are derived directly from the classification, codewords, and special handling instructions contained in format line twelve. The TCC is used primarily by automated systems to prevent transmission of messages via circuits that have not been authorized to process that information. Where multiple special handling caveats are included in a single message, the most restrictive TCC will be assigned.

For additional information regarding TCCs, refer to DOI-103 paragraph 308 or DOI-102 section 2.

### **3.5.9.4 CRITIC**

Pursuant to the provisions of Section 102 of the National Security Act of 1947 and Executive Order 12333, the Director of Central Intelligence (DCI) issued DCID 6/2 (P), now DCID 7/4, which established policy and procedures for the handling of critical information. The reporting of critical information is made in short, specially formatted messages, called CRITICs. CRITICs contain all essential facts about an event or situation and may be issued by any U.S. Government official. CRITICs are transmitted by the fastest means available. Messages carrying the CRITIC designator are handled in accordance with the instructions contained in USSID CR1501 and are transmitted in a manner to ensure deliver within 10 minutes to appropriate National Foreign Intelligence Board member organizations, the Army, Navy, Air Force, Marine, Major Commands, and such other recipients as designated. The original CRITIC is addressed only to "DIRNSA", but will be automatically forwarded to a list of designated initial recipients. Additional information for CRITIC transmission, format, and handling are contained in USSID CR1501, DOI-103, and NSA Supplement to DCID 7/4 (CRITIC HANDBOOK).

#### **3.5.9.4.1 TRANSMISSION**

Considering the nature of the CRITIC message, every effort must be made to effect transmission over the fastest means available, consistent with security requirements. CRITIC messages which cannot be transmitted electrically will be returned immediately to the message originator for appropriate action. The means of transmission of CRITIC messages are indicated below in the preferred order:

1. Primary DSSCS facilities

2. OPSCOMM IAW USSD-508
3. U.S. Government owned or leased and operated communications systems equipped for on-line cryptographic operations.
4. Facsimile compatible with RICOH 3312 utilizing STU III.
5. Telephonic communications via NSTS or STU III.
6. Commercial carrier to the nearest point of entry into a U.S. Government owned or leased network.
7. Any other transmission means available, providing necessary security requirements are met.

#### 3.5.9.4.2 CRITIC MESSAGE FORMAT

A special format is prescribed for the CRITIC message because of the vital significance of critical information and the absolute necessity for providing the most expeditious handling possible. It is designed to permit use of a terminal mask in communications processing. The CRITIC message will contain the following format lines and elements:

Line 1 - Start of message (SOM) and channel designator and sequence numbers (CDSN)

Line 2 - Routing line consisting of the CRITIC precedence prosign "WW" and the routing indicator "YEKAAH" only.

Line 3 - Prosign "DE", the routing indicator of the station responsible for initial message preparation, the constant four digit station serial number "9999" preceded by the number symbol, and the file time.

Line 4 - Security warning operating signal "ZNY" and the special intelligence community prosign "MM" followed by the transmission control indicator. This line will always read "ZNY MMQAD" on CRITIC messages.

Line 4A - Director line "ZKZK WW ZZZ DE"

Line 5 - CRITIC precedence prosign "W", originator's date-time-group, followed by the abbreviated month and year, and the operating signal "ZYH".

Line 6 - Prosign "FM" and the designation of the originator.

Line 7 - Prosign "TO" and the addressee "DIRNSA"

Line 11 - Start of Text (SOT) line containing the operating signal "ZEM"

Line 12 - Security classification assigned by the originator with each letter separated by a space, codeword (when assigned), special or restrictive handling instructions, the designator "CRITIC" followed by a one-up number by year.

Line 12A - "QQQQ" Special delimiter used to separate

classification and special handling instructions from remainder of text.

Line 12B - Text - as expressed by the originator.

Line 15A - End-of-message (EOM) validation number "9999" preceded by a number symbol.

Line 16 - EOM function

The following examples illustrate the proper sequence of elements in message preparation:

```

Line 1 - ZCZCLAA016
Line 2 - WW YEKAAH
Line 3 - DE YDHSLA #9999 011120
Line 4 - ZNY MMQAD
Line 4A - ZKZK WW ZZZ DE
Line 5 - W 022229Z JAN 07 ZYH
Line 6 - FM USN-24
Line 7 - TO DIRNSA
Line 11 - ZEM
Line 12 - C L A S S I F I C A T I O N CRITIC 1-2007
Line 12A - QQQQ (OPTIONAL)
Line 12B - TEXT
          DRV FM: DIRNSAM 123-2, DTD 24 FEB 1998
          DECL ON: X1, X3, X5, X6, X7, X8
Line 15 - #9999

Line 16 - NNNN

```

#### 3.5.9.4.3 CRITIC ACKNOWLEDGEMENT - RELAY STATIONS

Automatic relay stations will insure that the CRITIC message is transmitted to the NSACSS Communications Center by the most direct route. Relay stations will immediately acknowledge the receipt of a CRITIC message. This message is an acknowledgement for the originator of the CRITIC message that their message was received by the relay station. The acknowledgement message format is as follows:

```

ZCZCAKA023
ZTTMZYVW YEKHSV 0025 1232100-MNSH--YEKAKA.
ZNYMMNSH
ZYH
ZEM
SVC R W YEKAKA 0034 1122059
#0025

```

NNNN

#### 3.5.9.4.4 CRITIC HANDLING PROCEDURE - RELAY STATIONS

Each DSSCS Communications Center originating or relaying a CRITIC message will submit a report containing handling data incident to the message. This includes retransmissions as a result of ZES-2 actions, ZFG, and retransmissions due to non-receipt of QSL for the previous transmission. All communications centers are expected to provide accurate timing devices and maintain records which will reflect the exact handling times to the nearest second for CRITIC messages.

The CRITIC Handling Report will be filed two hours at routine precedence after transmission of a CRITIC message. For 24-hour stations, if more than one CRITIC message is transmitted during a single radio day, the report maybe filed, at the end of that radio-day, to include each transmission of a CRITIC message. The handling report will contain:

1. Message identification data (Originator and date-time-group)
2. All originators will indicate the time (to the nearest second) the operator began processing the CRITIC. Stations using automated systems, which assign the file time, are to report the time (to the nearest second) the message processing began, not the file time.
3. Routing indicator of the station to which the CRITIC was directly transmitted to and the time (to the nearest second) the message was completely transmitted.
4. Explanation for any delay exceeding three minutes encountered while handling the message, or any change in the date-time-group or file time.

The following is an example of a CRITIC handling report:

```
ZCZCLAA039
RTTMZYVW YDHLSA 0144 022349-MNSH--YEKAAH YEKVDH.
ZNY MMNSH
ZKZK RR XOA DE
R 010344Z JAN 2007
FM USN-24
TO DIRNSA//K04/X231//
INFO NNWC IOD MD//FN3//
ZEM
C L A S S I F I C A T I O N
QQQQ
SUBJ: CRITIC HANDLING REPORT FOR 01 JAN 07 RCS NSA-972
1. USN-24 010045Z JAN 07
2. 0010045:45
3. YDHA 0046:55Z
4. N/A
DRV: FM DIRNSAM 123-2, DTD 24 FEB 1998
DECL ON: X1, X3, X5, X6, X7, X8
#0101
```

NNNN

### **3.4.10 JOINT MESSAGE PREPARATION SYSTEM (JMPS)**

Also known as Message Editor provides the user with the ability to generate, edit, validate, address and save messages. The most often-used message types are USMTF, which is character based and Variable Message Format (VMF), which is binary.

### **3.5.11 COMMON MESSAGE PROCESSING (CMP) APPLICATION**

CMP is a United States message text format (USMTF) editor. The application makes it possible for a person to write a Naval Message with little knowledge of naval messaging. CMP aids the drafter with rules and procedures. CMP provides the correct formats for both man and machine and validates each message to ensure the message text conforms to MIL-STD-6040.

## **3.6 LOGS AND FILES**

### **3.6.1 GENERAL**

This section addresses the task of logging and file maintenance in an automated environment. Ashore and afloat automated systems have been developed which format and route messages and automatically accomplish the task of message logging, storage and retrieval. The requirement to maintain these logs and files are applicable in all automated telecommunications facility, although the media that records the information will be different.

The records and reports described herein are those necessary for effective communications and for monitoring and analyzing specific phases of communications. Requirements for additional logs, files, and reports must be carefully weighed. It cannot be emphasized too strongly that records, for their own sake, dilute unnecessarily the communications capability of the command and are detrimental to otherwise efficient communications.

Erasures to logs are not allowed. If corrections are made, the incorrect entry will be crossed out with one line so that the original entry is legible. The operator's initials will be affixed beside the correction or in the right hand margin.

Whenever an operator works on a circuit, that person's name will appear printed or typed in the appropriate log. The operator is also required to sign the log upon relief or when the circuit is secured.



### 3.6.2 MASTER STATION LOG (MSL)

The MSL is the official narrative record maintained to record significant events (e.g., power failures, complete system outages, major equipment outages or impairments such as HAZCON'S and any other event that may have an impact on operation), time verification, shift or watch changes, special tests, etc. Every Communication space must maintain a MSL.

Entries must be made in chronological order. The shift supervisor is required to sign the log when logging "on" and "off" duty and at the end of the RADAY.

If the MSL is an automated log, the system should use passwords and require the shift supervisor to log "on" and "off" duty. The supervisor's password serves as his/her signature. It shall also be designed so that it does not allow alterations.

A hard copy of the MSL must be filed at the end of each RADAY. The MSL shall be maintained for 12 months.

### 3.6.3 CENTRAL MESSAGE LOG

Depending upon the traffic volume processed by the command, either a separate incoming/outgoing or a combined central message log may be used to record traffic processed by the telecommunications facility. At a minimum, the originator, date-time-group, precedence, classification and time of receipt (incoming) or time of file and time of delivery (outgoing) should be logged for each message. The CML identifies which circuit or manner (for over the counter delivery) the message was relayed; this will prove helpful during tracer situations.

### 3.6.4 TOP SECRET CONTROL LOG

Upon receipt of a TOP SECRET, including all types of TOP SECRET SPECAT, addressed to the parent command or subscriber of the telecommunications facility, the center will assign a sequential number and enter the originator, date-time-group and copy count of the message into a log. A separate entry will be made for each customer addressed. The messages will be annotated "Copy\_\_\_\_\_of\_\_\_\_\_" and "Page\_\_\_\_\_of\_\_\_\_\_".

### 3.6.5 CIRCUIT LOGS

Records of messages transmitted via ship/shore circuits, whether primary ship/shore, full period termination, etc., must be maintained to ensure continuity of traffic, accurate times of delivery/receipt and precise files for possible tracer action. The preferred form to use is OPNAV FORM 2110-15, shown

in Figure 4-2, and is available through normal supply channels. Although OPNAV FORM 2110-15 is primarily designed for circuit receive side, only a pen-and-ink change is necessary to use it as a transmission log.

CIRCUIT		DATE	CARD NO.
S-T			
1		26	
2		27	
3		28	
4		29	
5		30	
6		31	
7		32	
8		33	
9		34	
10		35	
11		36	
12		37	
13		38	
14		39	
15		40	
16		41	
17		42	
18		43	
19		44	
20		45	
21		46	
22		47	
23		48	
24		49	
25		50	

FRONT

**STOCK NO. 0107-LF-704-6000**

**Send/Receive Message Log  
Figure 3-2**

**3.6.6 BROADCAST CIRCUIT NUMBER LOG AND RECORD DESTRUCTION**

Figure 4-3 is the check-off sheet used for keeping a record of broadcast numbers received onboard an afloat vessel or transmitted from a shore facility if accountability is being tracked via NCTAMS OTAM utilizing DUSC fleet center personnel IOT ensure effective delivery of message traffic to afloat units. This form provides for the number transmitted and received, the classification of the message. These forms may be reproduced locally. A similar form is available through supply channels (Stock number 0196-LF-301-8350).

**Broadcast Circuit Number Log & Record of Destruction**

BCSR No. CLASS	BCSR No. CLASS	BCSR No. CLASS	BCSR No. CLASS
01 U E C S T	26 U E C S T	51 U E C S T	76 U E C S T
02 U E C S T	27 U E C S T	52 U E C S T	77 U E C S T
03 U E C S T	28 U E C S T	53 U E C S T	78 U E C S T
04 U E C S T	29 U E C S T	54 U E C S T	79 U E C S T
05 U E C S T	30 U E C S T	55 U E C S T	80 U E C S T
06 U E C S T	31 U E C S T	56 U E C S T	81 U E C S T
07 U E C S T	32 U E C S T	57 U E C S T	82 U E C S T
08 U E C S T	33 U E C S T	58 U E C S T	83 U E C S T
09 U E C S T	34 U E C S T	59 U E C S T	84 U E C S T
10 U E C S T	35 U E C S T	60 U E C S T	85 U E C S T
11 U E C S T	36 U E C S T	61 U E C S T	86 U E C S T
12 U E C S T	37 U E C S T	62 U E C S T	87 U E C S T
13 U E C S T	38 U E C S T	63 U E C S T	88 U E C S T
14 U E C S T	39 U E C S T	64 U E C S T	89 U E C S T
15 U E C S T	40 U E C S T	65 U E C S T	90 U E C S T
16 U E C S T	41 U E C S T	66 U E C S T	91 U E C S T
17 U E C S T	42 U E C S T	67 U E C S T	92 U E C S T
18 U E C S T	43 U E C S T	68 U E C S T	93 U E C S T
19 U E C S T	44 U E C S T	69 U E C S T	94 U E C S T
20 U E C S T	45 U E C S T	70 U E C S T	95 U E C S T
21 U E C S T	46 U E C S T	71 U E C S T	96 U E C S T
22 U E C S T	47 U E C S T	72 U E C S T	97 U E C S T
23 U E C S T	48 U E C S T	73 U E C S T	98 U E C S T
24 U E C S T	49 U E C S T	74 U E C S T	99 U E C S T
25 U E C S T	50 U E C S T	75 U E C S T	00 U E C S T

Signature of individual authorizing destruction	Rank	File or Service No.
---	------	---------------------

**NOTE:**

U = Unclassified E = Unclassified/EFTO C = Confidential  
 S = Secret T = Top Secret

NOTE: This form is not stocked in the Naval Supply System but may be reproduced locally.

STOCK NO. 0196-LF-301-8350  
**Figure 3-3**  
**BCST Circuit Number Log**

**3.6.7 MESSAGE FILES**

By definition a communications center file refers to a station's filing system that will be maintained through electronic measures by an automated system or media designed for storage retrieval. The automated system or media will contain, for immediate

retrieval for viewing, readdressing, forwarding or printing, copies of all messages originated by, addressed to or relayed by a communication center. These message files are maintained on whatever media the automated system is designed to support, hard drive, diskette, or CD. The purpose of these files is to provide a repository for information that is required for both communications management and service. In addition to messages, the files also contain information relative to the processing of the message by the communications center.

#### **3.6.8 FILE MAINTENANCE**

Maintenance of a complete communications center messaging filing system is necessary to ensure the capability to readily refer to any message transmitted or received by a command. In an automated environment file maintenance is managed through a thoroughly monitored rotated media source. With the installation and upgrading of afloat and ashore automated systems the need for immediate recall from a servicing shore command are no longer necessary.

#### **3.6.9 EMBARKED COMMAND FILES**

The necessity for maintenance of separate messaging files for the embarked commander is dependent upon the direction of that embarked staff's Communications Officer. If directed, all guidance applicable as delineated herein will be adhered to.

#### **3.6.10 COMMUNICATIONS CENTER MASTER FILE**

The communications center master file shall contain a copy of every message sent or received by the center, including visual or remote radio messages for which the main communications center assigned date-time-group. For automated filing, messages will be filed on hard drive, diskette, or CD. Separate incoming and outgoing communications center master files may be maintained at the option of the command concerned.

#### **3.6.11 CRYPTO CENTER FILE**

The cryptocenter file will contain a copy of each message sent or received by the telecommunications facility which is TOP SECRET, SPECAT less SIOP-ESI, or designated for special privacy regardless of classification. TICON/NATO traffic must be filed separately. Messages are to be in date-time-group order and fillers for these messages will be placed in appropriate files.

#### **3.6.12 BROADCAST FILE**

TOP SECRET messages addressed to the command will be filed as directed in paragraph 3.6.4. Ships and commands that have temporarily ceased copying the broadcast because of land line or message guard arrangements are not required to maintain a complete file of broadcast numbers for the period in which

delivery of traffic was affected through the guard arrangements.

### 3.6.13 RECORDS DISPOSAL

Central Message - Log 30 days  
Circuits - 5 days

Communications Center Master (either paper or LDMX/NAVCOMPARS journal tapes) - 30 days

Crypto center file - 2 years  
Crypto center Destruction Log - 2 years  
General Message - When canceled  
Intelligence Summaries - 10 days  
Master Station Log - 12 months  
Messages incident to distress or disaster - 3 years

Messages incident to or involved in complaint for which the command has been notified - 3 years

Messages of historical or continuing interest (when no longer needed for local reference these will be transferred to the Federal Records Center, Mechanicsburg, PA.

Activities in the Washington DC area will transfer these to the Federal Records Center, Alexandria, VA) - Permanently

Meteorological Maps and Summaries - 2 days  
SPECAT SIOP-ESI file - 60 days

Relay station monitoring tapes or page copies of outgoing messages and service desk rerun records (primary relay station log record of all messages) 30 days

Top Secret Control log - 60 days  
Visual station - 30 days  
Watch-to-Watch inventory - 30 days

**THIS PAGE INTENTIONALLY BLANK**

**CHAPTER 4****COMMUNICATIONS SECURITY****4.1 GENERAL**

COMMUNICATIONS SECURITY (COMSEC) is the measure and controls taken to deny unauthorized person(s) information derived from telecommunications and ensure the authenticity of such telecommunications.

Communications Security includes the following:

1. **Crypto Security.** A component of COMSEC that results from the provision of technically sound cryptographic system(s) and their proper use.
2. **Physical Security.** Physical measures designed to safeguard COMSEC material or information from being accessed or intercepted by unauthorized person(s).
3. **Transmission Security.** A component of COMSEC that results from the applications of measures designed to protect transmissions from interception and exploitation by means other than crypto analysis.
4. **Emission Security.** Protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from the interception and analysis of compromising emanations cryptographic equipment, Automated Information Systems (AIS), and telecommunications systems.

**4.2 COMSEC INCIDENT**

Any uninvestigated or unevaluated occurrence that has the potential to jeopardize the security of COMSEC material or the secure transmission of classified or sensitive government information; or any investigated or evaluated occurrence that has been determined as not jeopardizing the security of COMSEC material or the secure transmission of classified or sensitive government information.

**4.3 COMSEC INSECURITY**

A COMSEC insecurity is an incident that has been investigated, evaluated, and determined to have jeopardized the security of COMSEC material or the secure transmission of classified or sensitive information.

#### 4.4 CRYPTO MARKINGS

A marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. government or U.S. government derived information.

**Note:** When written in all upper case letters, "CRYPTO" has the meaning as stated above. When written in lower case as a prefix, "crypto" and "crypt" are abbreviations for cryptographic.

#### 4.5 COMSEC MATERIAL

COMSEC material consists of aids and hardware which secure telecommunications or ensure the authenticity of such communications. COMSEC material includes, but is not limited to the following: COMSEC key, equipment, ancillary devices, documents, firmware or software that embodies or describes cryptographic logic and other items that perform COMSEC functions. COMSEC material is divided into the following three categories:

1. Keying Material. A type of COMSEC aid that provides the means to encode or decode manual or auto-manual cryptosystems. Keying material includes paper, electronic, and non-paper items. Keying material may or may not be marked or designated "CRYPTO".
2. COMSEC equipment. Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and by reconverting such information to its original form for authorized recipients.
3. COMSEC related information. Includes policy, procedural, and general doctrinal publications, equipment maintenance manuals and operating instructions, call signs, frequency systems, and miscellaneous material not listed above.

#### 4.6 WATCH-TO-WATCH INVENTORY

Each watch supervisor is responsible for all COMSEC material, held by the watch section. Prior to assuming the watch the supervisor must ensure all accountable items listed on a watch-to-watch inventory are sighted. At a minimum, the watch supervisor will account for:

1. All COMSEC material, including equipment not permanently installed, which will be listed by short title, edition, and serial number. If the inventory contains effective edition



information of COMSEC keying material, classify the inventory at least CONFIDENTIAL. As new material is received by the watch section, add it to the inventory. When material is destroyed or returned to the EKMS Manager deletes it from the inventory using proper line out procedures per EKMS 1 (series).

2. List permanently installed COMSEC equipment and secondary variables by short title and account for by quantity. Otherwise, list each piece as a separate line item on the inventory and account for by serial number.
3. List COMSEC accountable publications by short title and serial number.

In conjunction with each inventory, page checks will be done on all unsealed keying material, except key tapes packaged in canisters, using local destruction records or other sources of disposition documentation. Additionally, those loose-leaf publications which require page checks at the change of watch will be specifically indicated on the watch-to-watch inventory.

To provide positive control of communication accountable items, each watch will jointly conduct the inventory. The signing of the watch-to-watch inventory by the relieving watch certifies that all items were sighted, the required page checks were conducted, and that the relieving supervisor is responsible for them. The off-going watch will resolve any discrepancies noted prior to being relieved and, if the discrepancy involves EKMS material, the EKMS Manager or Alternate will be notified immediately.

The watch supervisor and another appointed individual will conduct the watch-to-watch inventory. If any COMSEC material is on the inventory, the persons conducting the inventory must be qualified EKMS users per EKMS 1 (series). The inventory will contain the date, specific watch, e.g., 0700-1500, and signature or initials of the individuals conducting the inventory. Start a new inventory on the first day of each month and retain spent inventories at least 30 days for accounting and management purposes.

#### **4.7 CLEARANCE REQUIREMENTS**

In conjunction with official duties, the Commanding Officer and others in the command who require access to classified material will hold a security clearance equal to or greater than the classification of the material. If U.S. Citizens whose primary duties are not cryptographic require access to low-level CRYPTO material (operational codes, authentication systems, call sign ciphers), the material may be issued provided the EKMS Manager thoroughly instructs the personnel in handling and safeguarding

the material concerned.

#### **4.8 ACCESS TO NATO INFORMATION**

Provided they hold a national clearance greater than or equal to the comparable NATO classification, U.S. personnel may be granted access to NATO SECRET and NATO CONFIDENTIAL material and must be briefed per OPNAVINST C5510.101. The following information is extracted from this instruction:

1. The phrase "NATO" signifies that a document is the property of NATO and must not be passed outside of the NATO organization;
2. All NATO information that is TOP SECRET bears the designation "COSMIC". For all other classifications, the phrase "NATO" will be applied to all copies of SECRET, CONFIDENTIAL, RESTRICTED, and UNCLASSIFIED documents prepared for circulation within the North Atlantic Treaty Organization. Under no circumstances should "NATO" be applied to U.S. documents;
3. The provisions of the Espionage Laws, Title 18, U.S. Code, Section 793, 794, and 798 are applicable to all classified NATO information;
4. All classified NATO information will be handled, stored, and accounted for per OPNAVINST C5510.101.

#### **4.9 CRYPTO ACCESS**

Resident aliens who are U.S. Government civilian, military, or contractor personnel that have been lawfully admitted into the U.S. and have been granted a final clearance based on a background investigation may be granted access to COMSEC material classified no higher than CONFIDENTIAL.

Foreign nationals will NOT be granted access to or provided information about COMSEC keying material without written permission from the material's controlling authority. Access to other COMSEC material must be approved by the National Security Agency.

Further access information for security guard(s), industrial personnel, and contractor personnel is detailed in EKMS 1 (series).

##### **4.9.1 TWO PERSON INTEGRITY (TPI)**

TPI requires the participation of two people to provide a means

of restricting access to sensitive material. When dealing with CRYPTO it requires at least two people, with authorized access to keying material. They must be in constant view of each other and the COMSEC material requiring TPI whenever the material is accessed and handled. Each person must be capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

To support TPI, specifically designed storage with two approved combination locks, each with a different combination with no one person authorized access to both combinations is to be employed. TPI locks must be General Service Administration (GSA) approved.

TPI is required in the following circumstances:

1. All TS paper keying material marked or designated CRYPTO
2. TS electronic key in an unencrypted form whenever it is:
3. Generated
4. Transferred
5. Relayed or received (OTAT)
6. Fill Devices (FD) with unencrypted TS key.
7. Unloaded FD in an operational communications environment containing keyed crypto from which TS key may be extracted.
8. Equipment that generates and allows for the extraction of TS keys.
9. Certified key variable generator equipment (e.g., KGV 99/99A or KG 83) is installed for operational use.

#### **4.10 ACCESS TO CLASSIFIED COMMUNICATIONS SPACES**

The Commanding Officer/Officer in Charge, having control over classified communication spaces, is responsible for controlling the access thereto, with access limited to persons who have a need to know. Clearance, rank or position does not, in themselves, entitle any individual to have access to CRYPTO or classified communication spaces.

Personnel authorized to process on-line and off-line record communications are commissioned officers and enlisted personnel (including non-rated) who possess an appropriate security clearance and have been specifically designated in writing by the officer in command. Federal Civil Service personnel who are employees of the Department of Defense may also be designated. Written designation and certification of personnel to process on-line and off-line communications may be effected by a locally generated administrative procedure.

Close and continuous supervision of classified communications by a commissioned officer is required. The choice of either his physical presence or availability on call is a matter for command determination. In aircraft, a commissioned officer or crewmember qualified in the applicable cryptosystems will be assigned

responsibility for supervising the use of crypto material authorized for operational use in aircraft. The authorizing command; however, will ensure proper crypto security, training and authorization of cognizant crew personnel as cryptographers prior to commencement of flight(s) which involve classified communications. Exceptions to the above rules follow:

1. Chief petty officers or petty officers in charge of small ships/craft or activities will be responsible for classified communications.
2. Operation of authentication systems, "couple codes," numeral and operational codes, and use of recognition signal extracts do not require continuous supervision by commissioned officers.
3. Under provisions of the Geneva Convention (1923), no member of the Medical, Dental, Medical Service, Nurse, Chaplain, or Hospital Corps will be assigned duties involving message processing in classified communications spaces. For small activities where the only commissioned officers attached are members of these service corps, the supervision of classified communications will be the responsibility of the chief petty officer or petty officer assigned to communications duties.

The following personnel not regularly assigned duty in classified communication spaces may be authorized access by the Commanding Officer/Officer in Charge without escort:

1. Command cryptographic maintenance personnel who may be admitted to spaces where crypto aids are stowed or are in use in the performance of their duties.
2. Cryptographic Repair Facility (CRF) personnel presenting appropriate credentials may be granted access, as applicable.
3. Special agents of the Naval Intelligence Command, conducting technical countermeasures surveys, are considered to have a legitimate need-to-know and may be granted access under normal operating conditions when security clearances and access authorizations are properly certified. Access to classified keying material and messages will be kept to a minimum consistent with the efficient conduct of the survey. Discussion about or access to classified information, crypto material and cryptographic operations will be limited to the extent consistent with the individual's need-to-know.

For maintenance or repair of spaces and non-cryptographic equipment, persons may be granted access to classified communication spaces provided they are sanctioned by the Officer-in-Charge and also escorted by authorized personnel. Escorts will ensure that these persons do not see any classified material

or cryptographic material/operations.

#### **4.11 ACCESS AND VISITORS CONTROL**

Maintain a master list of individuals having routine access to classified communications spaces. At a minimum this list should show the name and rank of authorized personnel, level of clearance and access authorized, as well as their specific function/spaces, e.g., fleet center, tech control, message center. Post the master list, or excerpts if more appropriate, conspicuously and near the entrance to classified communication spaces. Update the list whenever a personnel change occurs which affects the contents. Destroy superseded lists immediately.

Maintain a visitor log reflecting the following information:

1. Date
2. Visitor's printed name
3. Rank/rate/civilian
4. Organization
5. Purpose of visit
6. Visitor's signature
7. Person authorizing visit (signature)
8. Escort's name
9. Time in
10. Time out

Retain registers on file for two years after the date of the latest entry.

#### **4.12 SAFE COMBINATIONS**

Safe combinations to security containers are to be known only by those appropriately cleared persons who are authorized access to the classified information stored within and who must have the combination for efficient operation. Change combinations at least annually or sooner if the combination has been compromised or an individual who holds the combination transfers from the command or otherwise no longer requires it.

Per SECNAV M-5510.36, maintain a record for each security

container which shows the location of the container plus the name, home address and home phone number of each individual authorized to hold its combination.

#### 4.13 CLASSIFIED STORAGE

SECNAV M-5510.36 (June 2006) and EKMS 1 (series) provide information on the storage of classified material. COMSEC material, including keying material, equipment and publications, will be stored separately from other classified material, e.g., in separate containers, drawers or compartments within drawers. Unless the COMSEC material is under the direct control of persons authorized to use it, the containers or spaces will be kept locked.

#### 4.14 BEADWINDOW

BEADWINDOW is a real-time procedure which brings to the immediate attention of circuit operators the fact that an EEFI (Essential Elements of Friendly Information) disclosure has (or may have) occurred. The BEADWINDOW technique uses a code word and a number combination which is transmitted immediately by any net member to the unit disclosing the EEFI. At no time will the validity of the BEADWINDOW be discussed on the net. Proper response for a net member receiving a BEADWINDOW will be "ROGER OUT" using proper net call signs.

Standardized EEFI are established to identify specific items of information which, if acquired by an adversary, would degrade the security of military operations, special projects, etc. As a means to rapidly identify an EEFI violation on an uncovered radio telephone circuit, the BEADWINDOW code was developed to provide a means for immediate notification of insecure practices. The following standardized EEFI listing and associated BEADWINDOW code is promulgated for Navy wide implementation. The EEFI list will be posted in clear sight of operators at all insecure voice positions for rapid reference.

<u>BEADWINDOW</u> <u>CODE</u>	<u>EEFI</u>
POSITION 01	Friendly or enemy position, movement or intended movement: position; course; speed; altitude; or destination of any air, sea or ground element unit or force.
CAPABILITIES 02	Friendly or enemy capabilities or limitations: force composition or identity; capabilities, limitations or significant casualties to special equipment, weapon systems, sensors, units or personnel; percentages of fuels or ammunition remaining.

OPERATIONS 03	Friendly or enemy operations, intentions, progress or results: operational or logistic intentions; assault objectives; mission participants; flying programs; mission situation reports; results of friendly or enemy operations.
ELECTRONIC WARFARE 04	Friendly or enemy EW/EMCON intentions, progress or results: intention to employ EMC; results of friendly or enemy ECM objectives of ECM; results of friendly or enemy ECCM; results of ESM; present or intended EMCON policy; equipment effected by EMCON policy.
PERSONNEL 05	Friendly or enemy key personnel: movement or identity of friendly or enemy flag officers; distinguished visitors; unit commanders; movements of key maintenance personnel indicating equipment limitations.
COMSEC 06	Friendly or enemy COMSEC breaches: linkage of codes or code words with plain language; compromise of changing frequencies or linkage with line numbers/circuit designators; linkage of changing call signs with previous call signs or units; compromise of encrypted/classified call signs; incorrect authentication procedure.
WRONG CIRCUIT 07	Inappropriate transmission: information requested, transmitted or about to be transmitted which should not be passed on the subject circuit because it either requires greater security protection or is not appropriate to the purpose for which the circuit is provided.
08	For NATO assignment as required.
09	For NATO assignment as required.
10	For NATO assignment as required.
11-29	Reserved for COMUSNAVEUR.
30-49	Reserved for COMUSFLTFORCOM.
50-69	Reserved for COMPACFLT.

**Figure 4-1**  
**Beadwindow codes**

#### 4.15 ROUTINE DESTRUCTION PROCEDURES

Destroy classified material per SECNAV M-5510.36 by a method which prevents later recognition or reconstruction of the information. Destroy COMSEC material by following the procedures described in EKMS 1 (series).

Unclassified material, including FOUO material, does not require complete destruction and should only be introduced into the destruction cycle when the Commanding Officer or higher authority deems it efficient.

Routine destruction of TOP SECRET material or any COMSEC material requires two appropriately cleared witnesses.

All other destruction of classified material requires one appropriately cleared witness. Witnessing officials should:

1. Fill out proper documentation to record destruction of TOP SECRET or COMSEC material (EKMS 1 series refers).
2. Account for burn bags numerically and burn bags according to the classification of the material contained.
3. Observe the complete destruction of the bags.
4. When possible, sift through the residue to ensure reconstruction of information is impossible.
5. Take precautions to prevent wind or draft from carrying away classified material or burning/charred portions of it.

#### 4.16 EMERGENCY DESTRUCTION

Emergency destruction plans shall be part of SOP's for all communications activities and any command holding EKMS material. These plans outline procedures to reduce the amount of classified material held, and realign storage so that should emergency destruction be required, it can be accomplished in an expeditious manner. The plan should consolidate directions for emergency destruction and delineate the priority for destruction by specifying the destruction order of COMSEC material, special access material and the other material per SECNAV M-5510.36 and EKMS 1 (series). Conduct and document training exercises regularly so that all personnel involved understand the objectives of the plan.

Emergency destruction plans usually consist of several index cards with typewritten or neatly printed instructions arranged in priority of destruction order. Each card should contain a short task for one or two persons to accomplish. In this way the watch



supervisor or other person in charge of emergency destruction can hand out cards to several persons who work simultaneously. The cards should emphasize designating personnel responsible for the destruction, what must be destroyed and what method is employed. Check and update cards often to reflect any changes. Additional information for developing emergency destruction plans is found in EKMS 1 (series) and SECNAV M-5510.36. EKMS visit teams will critique and answer questions about command emergency destruction plans during the EKMS assist visits.

Most commands use the newer generation of crypto equipment that are keyed/re-keyed electronically or by key tape. This equipment is normally unclassified unless keyed and are easy to "zeroize", making it feasible to include relatively large quantities of equipment on a single emergency destruction card. Consult EKMS 1 (series) for detailed instructions on emergency destruction planning.

#### **4.17 ELECTRONIC SPILLAGES**

An electronic spillage is defined as data placed on an IT system possessing insufficient information security controls to protect the data at the required classification. An electronic spillage resulting in the compromise of classified information is subject to the requirements of SECNAV M-5510.36

Navy Telecommunications Directive (NTD) 03-06 was published in May 2006. The NTD outlines the procedures for reporting electronic spillages and provides a process to ensure classified data is removed from the affected network. As of this writing there are three serials that have been published;

A - (Directs commands to contact NAVGNOSC at 757-417-6777),

B - (Directs what to do if a Blackberry device is involved)

C - (Directs commands to conduct a Preliminary Inquiry (PI) IAW SECNAV M-5510.36 and notify Security Managers of each spillage))

The procedures for reporting and the Command Action Form (CAF) can be found at the following website:

[https://www.infosec.navy.\(smil\).mil](https://www.infosec.navy.(smil).mil) (Documentation Tab / NETWARCOM / Electronic Spillages). When reporting electronic spillages use the following distributive email address NNWC\_SPILLAGES@NAVY.SMIL).MIL.

#### **4.18 OPERATIONS SECURITY (OPSEC)**

The premise of OPSEC is that the accumulation of one or more elements of sensitive/unclassified information or data could damage national security by revealing classified information.

Over the years it became increasingly apparent that OPSEC had uses in virtually every government program that needed to protect

information to ensure program effectiveness. OPSEC professionals modified and improved techniques based on experience gained with many different organizations and in areas far a field from military combat operations. Today, OPSEC is as equally applicable to an administrative or research and development activity as it is to a combat operation. If OPSEC is not integrated into sensitive and classified activities, chances are that our adversaries will acquire significant information about our capabilities and limitations.

#### **4.19 TEMPEST**

TEMPEST is the code name given to the investigation, study, and control of compromising emanations from telecommunications and automated information processing systems.

Emission security (EMSEC) is the component of COMSEC that results from all measures taken to deny unauthorized persons information of value that might be derived from interception and analysis of compromising emanations from crypto equipment and telecommunications systems. The operation of communications and information systems may result in unintentional electromagnetic emissions. Although communications equipment is designed and generally tested to reduce the possibility of such emissions, COTS equipment is not. Unintentional emissions are extremely susceptible to interception and analysis and may disclose classified information. Commanders must follow applicable regulations providing guidance on control and suppression of such emissions.

#### **4.20 EKMS TRAINING VISITS AND INSPECTIONS**

EKMS Training Visits: All DoN EKMS accounts are required to receive a EKMS A&A Training Visit every 18 months. It is HIGHLY RECOMMENDED and in the command's best interest to use the training and assistance provided by the team prior to deployments and when Manger(s) change.

EKMS Inspections: All DoN EKMS accounts must undergo a formal EKMS Inspection every 24 months. This inspection will be unannounced and conducted in accordance with the procedures contained in EKMS 3 (series). The ISIC/IUC is required to submit a quarterly report via message to NCMS N7 detailing the results of formal EKMS Inspections. The format for this report and further information are contained in EKMS 3 (series).

EKMS Managers are required to use the inspection manual (EKMS 3 (series)) quarterly to conduct a self-assessment of their account.

## CHAPTER 5

### SHIP / SHORE AND SHIP / SHIP COMMUNICATIONS

#### 5.1 INTRODUCTION

To effectively execute their mission, ships require extensive coordination with higher echelon commanders, other ships within the Strike Group, shore commands providing technological and material support, and participating Joint and Coalition forces. To maximize the probability for mission success, a myriad of systems and circuits exist to ensure all mission participants have the ability to plan, coordinate and collaborate throughout the world. These C4I systems and circuits include SATCOM, Line-of-Sight UHF, VHF, HF, LF and VLF capabilities. They include voice, data and video communications both internal and external to the Strike Group. To facilitate world-wide access to these capabilities, Navy shore communications facilities have been segregated into specific AORs with the ability to cross-communicate.

##### 5.1.1 WORLD COVERAGE

Designated NCTAMS/NAVCOMTELSTA'S throughout the world guard ship/shore circuits to accept and relay traffic from afloat commands. The profusion of communications units guarding such circuits allows for virtually world-wide coverage for operating units by the Navy.

##### 5.1.2 CURRENT REGIONAL AREA OF RESPONSIBILITY CAPABILITIES

PAC AOR: The PAC AOR extends from approximately 105° east longitude to the western coast of the United States. Ships operating in the PAC fleet AOR receive primary communications support from NCTAMS PAC located at Wahiawa, HI.

SHF DSCS SATCOM can be terminated at three locations in the Pacific region: NCTAMS PAC Wahiawa, Ft Buckner, Okinawa Japan and Camp Roberts, CA. These three Teleport sites can support up to seventy-three (73) Navy missions simultaneously. The Regional Satellite Support Center (RSSC) will determine where each ship will be terminated by the resources at the Teleports and projected location and movement of the ship(s) within the region. When ships are establishing SHF termination services at non-Navy satellite communications facilities such as Camp Roberts or Fort Buckner, navy shipboard communicators must keep in mind that while these TELEPORT sites are operating similar to a NAVSATCOMFAC they are Army facilities without Navy communications personnel assigned and therefore do not have the benefit of navy

shipboard equipment knowledge and troubleshooting procedures. Navy communications personnel must review DISA directives, CIBS and procedures for SHF termination support to ensure proper configuration and testing requirements of termination path is met for timely and successful activation SHF transport services. Shipboard communications personnel must keep JFTOC informed of all efforts via COMSPOT reporting to ensure NCTAMS situational awareness and involvement in providing assistance to resolve SHF termination issues. SHF termination problems or casualties experienced must be documented in navy After Action Reports (AAR) and submitted via the C4I Access Request System (CARS).

Current CWSP architecture and infrastructure may be found on the NETWARCOM GLOBAL C4 READINESS website under the SATCOM CWSP link at the following URL: <http://c4spawar-chas.navy.smil.mil/global>.

The Global Broadcast System (GBS) primary injection point (PIP) and satellite broadcast management (SBM) center is located at NCTAMS PAC located in Wahiawa, HI and provides access to the UFO-8 satellite, which is equipped with five (four active, one spare) GBS transponders of 23.5 Mbps each, for a total of 94 Mbps per satellite. Data is transmitted to users from the satellite via three steerable spot beam antennas. Two of these cover an area of 500 nautical miles (nm) radius and support a nominal data rate of 23.5 Mbps. The third downlink is a wide spot beam that covers an area of about 2,000 nm radius and supports a data range of 12-23.5 Mbps.

Inmarsat-B HSD service in the PAC AOR is provided by three satellites, the 109E (Indian Ocean region (IOR)), 142W (Pacific Ocean region (POR)), and the 143.5E (IOR) satellites. Ships operating from 20° east to the continental United States (CONUS) operate through the 142W (POR)/143.5E (IOR) satellite with commercial SATCOM land Earth station (LES) at Auckland, NZ, and are also terminated at NCTAMS PAC. Inmarsat connectivity is constrained at three levels: NCTAMS termination equipment, terrestrial connectivity limitations, and available satellite channels. The existing infrastructure at NCTAMS PAC can accommodate a maximum of 70 Inmarsat-B HSD terminations (54 voice/data and 16 data-only terminations). The LES is, by contract, capable of landing 50 legacy 64 kbps channels. The existing terrestrial connectivity infrastructure (three T-1s) (T1 = 1.544 Mbps data throughput) is capable of supporting up to 72 legacy 64 kbps Inmarsat-B HSD terminations from the LES at Auckland, NZ, supporting the 109E (IOR) with 24 leases, 142W (POR) with 30 leases, and 143.5E (IOR) with 8 leases of satellite service. NCTAMS PAC has a theoretical channel capability of up to 66 channels. However, the USN is not the only customer competing for the assets, and therefore not all 66 may be available.

LANT AOR: Geographically extends from the east coast of the United States to approximately 5° west longitude where the United States Navy Europe (NAVEUR) Command AOR begins. Commander, Fleet Forces Command (COMFLTFORCOM) policy is that any Navy vessel

operating in the LANT AOR will terminate communications at NCTAMS LANT located in Norfolk, VA.

SHF DSCS SATCOM can be terminated at three locations in the Atlantic Region: NAVSATOCMFAC Northwest, Ft Belvoir and Ft Detrick. These three Teleport/STEP sites can support forty-two (42) Navy missions simultaneously. The Regional Satellite Support Center (RSSC) will determine where each ship will be terminated by the resources at the Teleport/STEP sites and projected location and movement of the ship(s) with the region.

Current CWSP architecture and infrastructure may be found on the NETWARCOM GLOBAL C4 READINESS website under the SATCOM CWSP link at the following URL: <http://c4spawar-chas.navy.smil.mil/global>.

Inmarsat-B HSD service in the LANT AOR is provided by the 98W (AOR-W) with 30 leases on the satellite. The AOR-W satellite's footprint covers from 179° west, in the Pacific, eastward to 20° west in the Atlantic. It is anticipated that service via the AOR-W satellite will be used by the Atlantic Fleet only. Channels are supported by the commercial SATCOM LES at Laurentides, Canada, and terminated at NCTAMS LANT Norfolk, VA. Inmarsat connectivity is constrained at three levels: NCTAMS termination equipment, terrestrial connectivity limitations, and available satellite channels. NCTAMS LANT is outfitted with termination equipment to support 48 channels. The LES is, by contract, capable of landing 50 legacy 64 kbps channels. Current terrestrial connectivity (two T-1s) can support up to 48 legacy 64 kbps Inmarsat-B HSD terminations. NCTAMS LANT has a theoretical channel capability of up to 48 channels. However, the USN is not the only customer competing for the assets, and therefore not all 48 may be available. In all cases, the aggregate of the satellite links are backhauled over terrestrial links (commercial or Defense Information Systems Network (DISN)) to NCTAMS LANT for distribution to individual users or product sources. Obtaining terrestrial connectivity from the various SATCOM Earth terminals to NCTAMS LANT is low risk as the terrestrial connectivity is shore-based and within CONUS.

NAVEUR AOR: The NAVEUR AOR reaches from approximately 5° west to 35° east latitude. Commander, United States Naval Forces, Europe (COMUSNAVEUR) policy is that any Navy vessel operating in the NAVEUR AOR will terminate communications at NCTS NAPLES, ITALY.

SHF DSCS SATCOM can be terminated at two locations in the NAVEUR region: NAVSATCOMMFC Lago di Patria and Landstuhl GE. These two Teleports can support up to forty (40) Navy missions simultaneously. The RSSC will determine where each ship will be terminated by the resources at the Teleports and projected location and movement of the ship(s) within the region.

Current CWSP architecture and infrastructure may be found on the NETWARCOM GLOBAL C4 READINESS website under the SATCOM CWSP link at the following URL: <http://c4spawar-chas.navy.smil.mil/global>.

Inmarsat-B HSD service in the NAVEUR AOR is provided by the 25E (AOR-E) with 33 leases on the satellite. The AOR-E satellite footprint covers from 60° west, in the Atlantic, eastward to 100° east in the South China Sea. The satellite supports assigned users in the Mediterranean Sea, as well as the IO and the Persian Gulf. Channels are supported by the commercial SATCOM LES at Goonhilly, UK, and are terminated at NCTS NAPLES, ITALY Naples, Italy.

Inmarsat connectivity is constrained at three levels: NCTAMS termination equipment, terrestrial connectivity limitations, and available satellite channels. NCTS NAPLES, ITALY is equipped to terminate up to 50 Inmarsat-B HSD channels. The LES is, by contract, capable of landing 50 legacy 64 kbps channels. Current terrestrial connectivity (one E-1) between the LES and NCTS NAPLES, ITALY, however, limits the number of channels to a maximum of up to 50.

In all cases, the aggregate of the satellite links are backhauled over terrestrial links (commercial or DISN) to NCTS NAPLES, ITALY for distribution to individual users or product sources.

Obtaining terrestrial connectivity from the various SATCOM Earth terminals to NCTS NAPLES, ITALY can be problematic. Terrestrial connectivity for Inmarsat-B HSD and SHF SATCOM is handled in the AOR by either a commercial vendor or the DISN.

NAVCENT AOR: The Navy Component, Central Command (NAVCENT) AOR extends from approximately 35° east to 90° east longitude. NAVCENT policy is that any Navy vessel operating in the NAVCENT AOR will terminate communications at NCTS Bahrain.

SHF DSCS SATCOM can be terminated in three locations in the NAVCENT region: NAVSATCOMMFAC Lago di Patria, Landstuhl GE, and NCTS Bahrian. These three Teleport/STEP sites can support up to thirty-three (33) Navy missions simultaneously. The Regional Satellite Support Center (RSSC) will determine where each ship will be terminated by the resources at the Teleport/STEP sites and projected location and movement of the ship(s) within the region.

Current CWSP architecture and infrastructure may be found on the NETWARCOM GLOBAL C4 READINESS website under the SATCOM CWSP link at the following URL: <http://c4spawar-chas.navy.smil.mil/global>.

The NAVCENT GBS PIP is located at NCTS Sigonella, Italy, and provides access to the UFO-10 satellite, which provides coverage to the NAVCENT region. The satellite is equipped with three GBS transponders at 30 Mbps each, for a total of 94 bps. Data is transmitted to users from the satellite via three steerable spot beam antennas. Two of these cover a 500 nm radius and support a nominal data rate of 30 Mbps. The third downlink is a wide spot beam that covers an area of about 2,000 nm radius and supports a data rate of 30 Mbps.

Inmarsat-B HSD service in the NAVCENT AOR is available from two satellites, the 25E with 33 leases (AOR-E) and 109E (IOR) with 24 leases on the satellites. The AOR-E satellite footprint covers from 60° west, in the Atlantic, eastward to 100° east in the South China Sea; the IOR satellite footprint covers from 30° east, in the eastern Mediterranean Sea, eastward to 107° west in the Pacific. AOR-E channels are supported by the Goonhilly, UK, LES and terminated at NCTS Bahrain. IOR channels are supported by the Auckland, NZ, LES and are terminated at NCTS Bahrain. Typically, Inmarsat-B HSD-equipped ships physically located in the Persian Gulf are terminated at Goonhilly, UK, and routed to Bahrain. Naval units in the IOR and not physically located in the Persian Gulf will normally be terminated with the Inmarsat LES located in Auckland, NZ. These terminations are forwarded to NCTAMS PAC Wahaiawa, HI, for distribution to users and product sources.

Inmarsat connectivity is constrained at three levels: NCTAMS termination equipment, terrestrial connectivity limitations, and available satellite channels. Two satellites, 109E and 25E support the NAVCENT AOR. As those satellites also have responsibilities to cover other AORs (25E in the Mediterranean and 109E in the IO) inter-fleet coordination may be required to meet the fleet's Inmarsat requirements. Current capacity is up to 48 channels via the 25E satellite, shared with Sixth Fleet requirements in the Mediterranean, and up to 66 channels via the 109E satellite, shared with Seventh Fleet requirements in the IO. The NAVCENT Inmarsat shore architecture provides a single T-1 between NCTS NAPLES, ITALY and the Indian Ocean region network operations center (IORNOC) in Bahrain to backhaul Inmarsat data.

### 5.1.3 PROBLEM AREAS

Several areas of the world are noted for difficulty in establishing ship/shore communications. Some of the more infamous areas are: north of 75 degrees north latitude and south of 60 degrees south latitude in the Atlantic Ocean, the Antarctic Ocean, the Indian Ocean; the extreme southerly portion of the South Pacific Ocean; the North Arabian Sea; and the area west of Norway. Prior to operating in these areas, contingency planning is vital to successfully overcome anticipated communications difficulties. If communications problems are encountered in these areas, the terminating NCTAMS can provide additional frequency support when requested.

### 5.1.4 UNAUTHORIZED TRANSMISSIONS

Unauthorized transmissions, especially those of obscene, indecent or profane nature, indicate a lack of good order, circuit discipline and transmission security. Such transmissions will not be tolerated on Navy circuits, be they voice or radio

teletypewriter circuits. The Federal Communication Act of 1934 addresses this violation and is quoted in part:

**"Whoever utters any obscene, indecent or profane language by means of radio communications shall be fined not more than \$10,000 or imprisoned not more than two years, or both."**

No person shall knowingly or willfully originate, accept, transmit, deliver, or cause to be delivered a spurious message or one falsely purporting to have been received by naval communications. Also, the use of profanity and obscenity in radio transmissions is prohibited and violators are subject to charges under the UCMJ. This is essential both to circuit discipline and compliance to Federal law.

As unauthorized and obscene transmissions are not usually accompanied by call sign identification or personal identifying information, extra effort must be exerted to identify the offending station. To accomplish this, the use of tape recorders, accurate log keeping, notes on offending operator characteristics, exact frequency measurements and directional finders (DF) bearings will help in proper identification. Monitoring will be performed per applicable OPNAV and SECNAV instructions.

Whether or not positive identification can be made, all incidents involving unauthorized transmissions, as noted above, shall be reported by the receiving or monitoring command to the appropriate Fleet Commander, with information copies to COMNAVNETWARCOM. All identifying information shall be enclosed with the report.

#### **5.1.5 VIOLATION REPORTS**

Both afloat units and shore stations are to bring deviations from prescribed procedures to the attention of violators via record message traffic. In the event of continuous flagrant violations, a speed letter report will be submitted to the FLTCOM's, with copies to COMNAVNETWARCOM, the type commander, and the offending afloat unit/communications station. The report will include a description of the violation, publication reference and date/time of violation.

#### **5.1.6 HARMFUL INTERFERENCE - COMMUNICATIONS JAMMING, IMITATIVE COMMUNICATIONS DECEPTION**

Harmful interference is defined in the ACP 121-series. The saturated frequency spectrum, caused by the increasing worldwide use of radio communications by governments and commercial concerns, has created a situation wherein interference can be expected and often must be tolerated. Thus, stations



experiencing interference should initially consider such disruption of communications to be interference rather than jamming and take appropriate action per ACP 121-series. Reports of US interference to the communications facilities of other nations should be handled expeditiously.

Communications jamming is the deliberate radiation, re-radiation, or reflection of electromagnetic signals with the object of impairing or denying the use of communications circuits by the enemy. This is accomplished by the transmission of electromagnetic signals to enemy receivers. In jamming operations, the signals produced are intended to obliterate or obscure the signals the enemy is attempting to receive. Signals whose modulation characteristics or manner of keying is clearly for the purpose of obstructing a radio channel should be assumed to be jamming. Jamming signals will usually be changed in frequency to follow changes in frequency on the circuit experiencing the jamming.

Some common forms of communications jamming are:

1. Several carriers adjusted to the victim frequency. Each carrier amplitude modulated by a nonsinusoidal frequency.
2. Simulated traffic handling on the victim frequency.
3. Random noise amplitude modulated carriers.
4. Random noise frequency modulated carriers.
5. Continuous wave carrier, (keyed or steady).
6. Several audio tones used in rapid sequence to amplitude modulate a carrier (bagpipe).

Measures to counter and minimize the effect of jamming shall be employed in the order listed:

1. Prepare instructions and procedures to be followed (including alternate routing of traffic) on circuits most susceptible to jamming.
2. Request sending stations to continue live traffic on jammed circuits to create the impression that jamming is ineffective.
3. Check tuning of receiver. Request the sending station to check tuning of transmitter on the jammed circuit. Various receivers differ both in the degree of selectivity afforded for close discrimination between signals whose frequencies are very near to each other and in the circuitry used to reject or limit unwanted signals. Therefore, maximum

advantage should be taken of all receiving facilities available for selection of those best suited for operation under the type of jamming being experienced.

4. Ensure correct bearings and maximum efficiency of directional antennas, for both receiving and transmitting, when available. It is probable that the true bearings of desired and jamming signals will differ considerably. Advantage should be taken of the radiation patterns of the various installed antennas for selection of the antenna most favorable to reception of the desired signal and to transmitting the strongest signal in the desired direction. Most antennas have some directional effects, even when intended to be omni-directional.
5. Use panoramic adapters, if available. The visual display of the frequency spectrum in which jamming is being experienced makes available the means for precisely monitoring changes in tuning and in selecting clear channels, and aids in submitting the required report of jamming.
6. Request sending station to increase power. This request shall be classified, unless an alternate radio net is available, in which case an unclassified request may be made if the tactical situation dictates.
7. Request sending station to shift frequency. Consult propagation publications to determine if there is a better frequency available for transmission path involved. The request for a frequency shift shall be classified unless an alternate radio net is available, in which case an unclassified request may be made if the tactical situation dictates. Live traffic, operator's normal signals, and so forth, must continue on jammed circuits if a frequency shift is made.
8. Divert low-precedence traffic from radio channels to mail or courier.
9. Anticipate further shifts in frequency. The new primary frequency must be supported by having its secondary placed in a standby condition.

Imitative communications deception is the introduction of fraudulent transmissions, in imitation of authentic transmissions, into enemy communications systems for the purpose of confusing or deceiving. (see ACP 122 (series) for descriptive data and defensive measures concerning imitative communications deception.)

Incidents of harmful interference, communications jamming and imitative communications deception will be reported per OPNAVINST C3430.18.

**5.1.7 COAST GUARD HF SHIP / SHORE CIRCUITS**

Coast Guard Ship/Shore circuits are available for use by U.S. Navy Vessels during times when satisfactory communications cannot be maintained with their servicing NAVCOMTELSTA and High precedence traffic needs to be delivered. Coast Guard COMMSTA's have access to AUTODIN for further delivery of traffic to message addressees.

Coast Guard COMMSTA's with HF Ship/Shore circuits compatible with U.S. Navy HF systems can be contacted on SSB Voice for initial circuit coordination. Calling and working for Ship-Shore-Ship communications will be in the duplex frequency mode. Frequencies shown below are window frequencies.

**Current HF on call services for CG Communications Area Master Stations (CAMS) and COMMSTA Kodiak Alaska:****HF On Call Services at CAMSLANT (NMN):**

Air to Ground - 5696khz, 8983khz, 11202khz (On request), and 15088khz

COTHEN - CG Scan list

Secure Air to Ground and/or Secure Vox: Contact CAMSLANT via above freqs to coordinate

GMDSS - (associated DSC) vox freqs - 2182khz, 4125khz, 6215khz, 8291khz, 12290khz (1100Z- 2300Z), and 16420khz (on request)

Autositor - CAMSLANT/Boston/New Orleans/Miami Xmit freqs

4210.3  
6314.3  
8426.3  
12590.8  
16817.8  
22387.8

CAMSLANT/Boston/New Orleans/Miami RCV freqs

4172.3  
6262.8  
8386.3  
12488.3  
16694.8  
22295.8

**HF On Call Services at COMMSTA Kodiak (NOJ):**

2182 kH International Distress/Initial Contact Frequency - silent periods enforced.

2670 kHz working frequency used for NOJ WX Broadcasts (may be used if no traffic or broadcasts at that time)

4125 kHz frequency is used for distress, NWS WX Broadcasts, Safety and Urgent marine broadcasts, Vessel observations, etc.

6215 kHz Distress/Initial contact

6501 kHz Voice Automated WX Broadcast (VOBRA) (may be used if no weather broadcast at that time)

5696 kHz Air to Ground frequency

8983 kHz Air to Ground frequency

11202 kHz Air to Ground frequency  
Secure Air to Ground and/or Secure Vox: contact COMMSTA Kodiak via above freqs to coordinate

SITOR FREQUENCY GUIDE

Transmit

SITOR 1	6315.8	24HR
SITOR 2	8417.8	DAY
SITOR 3	4211.8	NIGHT

Receive

SITOR 1	6264.3
SITOR 2	8377.8
SITOR 3	4173.8

DSC FREQUENCY GUIDE

Transmit

Receive

2185.8	2187.5
4205.8	4207.5
6310.3	6312.0
8412.8	8414.5
12575.3	12577.0
16802.8	16804.5

List of ALE frequencies

CH 1. 3053.0	CH 2. 4730.0	CH3. 6709.0
CH 4. 9034.0	CH 5. 11196.0	CH 6. 13221.0
CH 7. 15082.0	CH 8. 17988.0	CH 9. 20135.6
CH 10. 23072.6		

**HF On Call Services at CAMSPAC (NMC) :**

VOX - 4125/6215/8291/12290

Air to Ground - 5696/8983

Secure Air to Ground and/or Secure Vox: contact CAMSPAC via above freqs to coordinate

## SITOR:

## CAMSPAC SITOR

8414.8 mhz

16804.8 mhz

## Honolulu SITOR

8414.8 mhz

12577.3 mhz

22374.3 mhz

## Guam SITOR

12577.3 mhz

16804.8 mhz

22374.3 mhz

To achieve compatibility with equipment of other than U.S. Navy forces, the following information and definitions must be understood:

1. There are three types of HF transmitters/ transceivers capable of SSB operation in general use by the U.S. Navy. These are the AN/URT-23, the AN/URT-24 and on LINK-11 equipped platforms, the AN/SRC-16.
2. Marine Corps single sideband radio equipment is limited to integral one kilohertz tuning increments of the operating band. (Example: 3036, 3037 and 3038 kHz).
3. Because of the stringent frequency tolerance of the teletype conversion equipment used in Marine Corps single sideband, it is necessary that Navy transmitters be maintained within plus or minus 15 hertz of the correct frequency.
4. Marine Corps single sideband equipment used on radio teletype circuits with Navy units employ 850 hertz frequency shift keying (FSK) in the upper sideband mode.
5. ASSIGNED FREQUENCY is the center of the authorized frequency bandwidth (intelligence band) assigned to a station. This is also the frequency for which clearance is requested when clearing frequencies for use in a specific area.
6. REFERENCE FREQUENCY is a frequency which has a fixed and specified position with respect to the assigned frequency.

7. SINGLE-SIDEBAND-SUPPRESSED-CARRIER-FREQUENCY. The carrier is virtually suppressed and not intended to be used for demodulation. This frequency is sometimes referred to as the reference frequency. In U.S. Navy Single-Sideband-Transmitters the carrier frequency, depending on the transmitter type, may be either offset from the assigned frequency or set on the assigned frequency.
8. In order to provide operational flexibility, a number of frequencies will normally be provided by the NCTAMS in conjunction with the FLTCOMs and numbered fleet commanders for pool use where required. Frequencies cleared for SSB only (2K80J3E or 3K00J3E/3K00J7B), will indicate the suppressed carrier frequency in parenthesis following the assigned frequency. Frequencies cleared for 300HF1B, as a general rule, will have a suppressed carrier frequency displaced 2 kHz below the assigned frequencies. In any case, instruction books for the particular equipment should be consulted to confirm the location of the suppressed carrier frequency.

Characteristics for FSK operation of the following radio sets are provided for your information. However, instruction manuals for specific equipment can be expected to be more thorough and current:

1. AN/URT-23/24. Emits the space and mark signal, plus 425 Hz and minus 425 Hz, centered on the dial frequency.
2. AN/TRC-75. Emits the space and mark signal, plus 425 Hz and minus 425 Hz, centered 2000 Hz into the upper sideband.

#### **5.1.8 HF INTERNET PROTOCOL/SUBNET RELAY (HFIP/SNR)**

The Navy Tactical Network program of record is an Increment II evolution of a very successful POR called HF Data Systems or HFDS. HFDS offered Allied/Coalition digital communications over HF in the form of Battle Force E-Mail or BFEM. A lowest-common-denominator system BFEM was intended to facilitate primarily ship-to-ship communications over an Extended Line of Sight radio environment with "point to point" links carrying e-mail (SMTP) traffic to and from US Navy ships into NATO communications environments. Its Operational Requirements Document called for an incremental increase in both platform interoperability (beyond just ships) and IP-enabled connectivity. Research investments by ONR and the program office results in a synergism of technologies across several RF pathways and IT interfaces to result in an extended range data communications system called HFIP/SNR.

The HFIP/SNR technology promulgates usefulness that is at once common and unique to each naval platform user (land, sea, surface, undersea and aerodyne). Common usefulness of this system

centers around a self-forming, self-repairing network capability with a highly secure digital communication range of 20-700 nautical miles, thereby eliminating the need for voice transmissions and satellite reach back; which can be time-consuming and susceptible to error. The HFIP Gateway system also takes advantage of radios already in place in aircraft, ships, shore stations and submarines, providing a means of relatively low-cost integration of IP information to the navy's Global Information Grid information environments (US Only and Allied/Coalition).

The currently fielded Navy Tactical Network or NTN is a network of many HFIP/SNR communication systems. On each platform the HFIP/SNR system is allocated to service either US only communications (SECRET) or Allied/Coalition (NATO SECRET). The HFIP/SNR systems are designed to allow platform to route IP data (chat, email, file transfers) over available High Frequency (HF) and Ultra-High Frequency (UHF) mediums to their respective aircraft, submarine, ship and shore ground counterpart sites in Token Ring (via HFIP) or TDMA (via SNR) networking topology. The HFIP H=Gateway also acts as a relay point to allow one HF connected node to relay IP traffic between two nodes that are not within HF communications distances.

The composition of each system varies based on their legacy HF/UHF radios and LAN infrastructure. Basically though each platform will have a "Controller" that performs the HF-UHF medium to IP data exchange, network access control, and packet directing duties through the use of functionally limited LINUX-based software; which operates on a standard Pentium II (or higher) Personal Computer (PC) with at least 256Mb of RAM, two Ethernet ports, and one Peripheral Component Interconnect (PCI) slot. Additionally, each "Controller" (one for HFIP and one for SNR functions) contains a synchronous board that provides control signals required to initiate modem and crypto synchronization preambles necessary to key the RF equipment. Both systems use a dedicated MIL-STD-188 based RF modem. A NIST certified Intrusion Protection/Intrusion Prevention Firewall is mounted between the platform's LAN components and these HFIP/SNR devices and a NSA Type I encryption device is mounted between the HFIP/SNR devices and the platform's designated RF transmitter and receiver radio equipment. Figure 5-1 depicts a typical HFIP/SNR System Architecture concept.

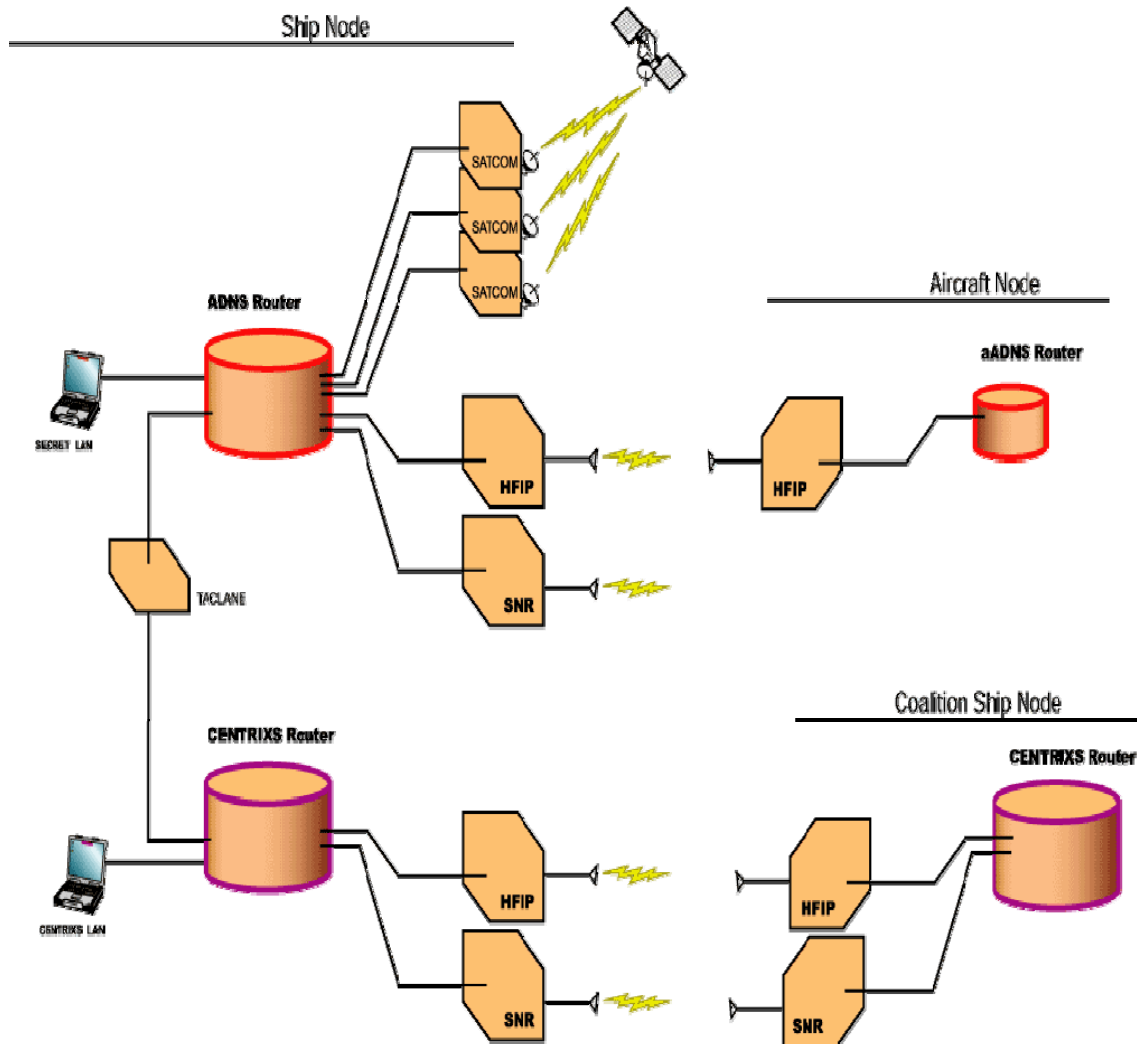


Figure 5-1  
HFIP/SNR Architecture

#### 5.1.9 AFLOAT ELECTROMAGNETIC SPECTRUM OPERATIONS PROGRAM (AESOP)

Electromagnetic Spectrum Operations Program (AESOP) is a computer program designed to automate frequency planning for radar and weapons systems as well as the process of generating communications plans. The Strike Group staff or designated frequency coordinator uses the radar planning component of AESOP to select frequencies and separation distances for the group's ships to ensure that the radars operate with a minimum of electromagnetic interference (EMI).

The communications planning component provides the communications planner with an automated method of drafting the OPTASK COMMS message. The OPTASK COMMS message is the means used by which the



United States Navy and Allied Navies distribute afloat communications plans.

To support Communication Planning in developing a Communications Plan, the AESOP database also contains:

- Platforms
- Communications Equipment
- Line Numbers
- Emission Designators
- Guard Keys
- Keying Material (KEYMAT)

Software functionality is taught in the Frequency Management, ICMC and IT schools. Students are taught how to create new platforms, add communications equipment, edit line numbers, emission designators, guard keys, and CRYPTO keymat.

AESOP is designed to execute on a Windows 2000/NT/XP based personal computer, and may be installed in either a stand-alone or a file sharing application. The software can be used to generate a new OPTASK COMMS or manipulate an existing one. The CNO has mandated that AESOP software must be used in all communications and RADAR plans development, modification and dissemination.

AESOP supports the multi-step process of developing a Communications Plan (COMPLAN) and promulgating it to appropriate recipients. Writing the OPTASK COMMS is a detailed process that encompasses many areas and concerns. In general, the following order is observed:

1. Customize the workspace by adding the units and hull numbers of participants.
2. Verify the communications equipment installed on each platform and update the database with current information.
- 3.
4. Establish a list of required nets.
5. Establish priorities for the nets by frequency band.
6. Determine the guard requirements.
7. Write and Transmit a Frequency Request Message to obtain frequencies.
8. When received, import the Frequency Assignment Message, populating the nets with their assigned frequencies.
9. Verify that the assigned frequencies meet required minimum separation criteria and are free of IMI.

10. Establish Frequency Guard Bands for frequencies that are not available.
11. Import Standard Frequency Action Format files from a standard frequency management database, such as FRRS.
12. Develop Aircraft Channelization Plans and DAMA Channelization Plans.
13. Generate and Transmit the OPTASK COMMS.
14. Publish the AESOP Spectrum Report for use by the IWC.

#### **5.1.10 FREQUENCY MANAGEMENT**

The Navy uses an area frequency management concept where the US and Possessions (US&P) is divided into areas for which the responsibility has been designated to Navy Area Frequency Coordinators or Commands.

One aspect of frequency management that is common to all DoD organizations is that the commander of an installation is responsible for management of the spectrum on the installation.

Many organizations are involved in Navy spectrum management to ensure mission success. As mentioned earlier, the Navy assigns coordinators, who operate on a regional and local basis and resolve frequency management and coordination issues within their respective geographic regions. Some of the coordinators are:

NMCSO LANT Norfolk  
 NMCSO EUR Naples  
 NMCSO CENT Bahrain  
 NMCSO PAC Honolulu  
 NMCSO NORTH WEST Puget Sound  
 NMCSO SOUTH WEST San Diego  
 NMCSO Guam  
 NMCSO FE Yokosuka

Authority for use of radio frequencies by USN and USMC activities within an area of responsibility is requested via the commander of the appropriate Navy component. The assignments are normally made by the FP to the theater commander.

Direct responsibility for managing Navy frequency use in international waters rests with the Numbered Fleet Commanders, who will obtain Department of the Navy (DoN) radio frequencies in quantities sufficient to sustain training and operations. Numbered fleets will manage and coordinate use of frequencies with NMCSO regional support centers; provide timely notification of frequency use; develop, maintain and promulgate standard Strike Group communications plans; and collaborate to develop,

maintain and promulgate Navy-Wide OPTASK COMMS. Numbered Fleets will require that forces operate C-E equipment within the parameters of the applicable frequency assignments.

Responsibility for managing Navy frequency use in foreign countries may rest with either the Senior Naval Force Commander or the Joint Forces Commander. Fleet forces can submit frequency request to the Numbered Fleet Commander in cases where additional frequencies are required. Numbered Fleet spectrum managers will promulgate specific instructions and procedures about how to obtain and use radio frequencies. Conservative use of the radio frequency spectrum is strongly encouraged to minimize the risks associated with interference, hostile jamming and intrusion.

#### **5.1.11 FREQUENCY RESTRICTIONS AND VARIOUS THEATER OF OPERATIONS**

Because the radio frequency spectrum is a limited natural resource, all radio frequency usage is restricted or regulated in some way. Responsibility for establishing base frequency restrictions rests with the base commanding officer. Base frequency managers will promulgate restrictions on a regular basis. Responsibility for establishing fleet frequency restrictions rests with the numbered fleet commander, who will develop, maintain and promulgate radio frequency restrictions, to include host nation restrictions where applicable, with the goal of reducing the likelihood of radio frequency interference.

### **5.2 SATELLITE COMMUNICATIONS**

#### **5.2.1 GENERAL**

In today's automated telecommunications environment, the primary means of Ship/Shore Communications is via satellite. Shore and shipboard satellite subsystems are in a continuing state of evolutionary development. CIB/CIA'S are apt to provide the best current information on the latest procedures for communicating in this dynamic environment. Current Satellite Communications (SATCOM) information is available using links from the NAVNETWARCOM C4I status page on the SIPRNET ([http://sgeminii.spawar-chas.navy.smil.mil/C4I\\_GlobalStatus/GlobalStatus.aspx](http://sgeminii.spawar-chas.navy.smil.mil/C4I_GlobalStatus/GlobalStatus.aspx)) Follow the links from the various spectrums to find information on current status, satellite assignments, user handbooks and other information.

#### **5.2.2 ULTRA-HIGH FREQUENCY (UHF) SATELLITE COMMUNICATIONS**

The Navy UHF SATCOM system provides reliable, long-haul communications services to Navy users operating a variety of terminal systems ranging from single channel equipment to complex

multiple subsystem terminals. UHF military satellite communications (MILSATCOM) systems provide capacity on demand for transport services that support a wide variety of applications including SECVOX, messaging, facsimile, secondary image transfer, packetized data service, and e-mail used during normal and contingency or crisis operations.

The UHF follow-on satellite system (UFO) is the predominant UHF system in use today. There are eight UFO satellites, each with 39 UHF channels per satellite: twenty-seven 25-kHz channels, twenty-one 5-kHz channels (Note: UFO-11 is equipped with four additional 5-kHz channels for a total of twenty-five 5-kHz channels), and one jam-resistant EHF uplink 25-kHz UHF downlink channel supporting either the fleet broadcast or the Integrated Broadcast System-Simplex (IBS-S). Seven UFOs are also EHF-capable; two UFOs are equipped with Ka-band GBS packages.

The UHF Constellation also includes 2 Fleet Satellite Communications (FSC) satellites. The first FLTSAT was launched in 1978 and the last in 1989. Of the original satellites, only FSC-7 and FSC-8 remained operational and are past their end-of-life. FLTSAT are considered as complementary element of the UHF MILSATCOM space segment. The satellites have four types of UHF communications channels for a total of 23 channels. There is a single broadcast channel (Ch 1), nine 25-kHz fleet relay channels (Ch 2-10), 12 Air Force 5-kHz channels (Ch 11-22) and one wideband, 500-kHz channel (Ch 23). All channels are UHF uplink and downlink.

Tactical circuits that are supported by UHF SATCOM include half-duplex voice (2.4 kbps) and data (2.4-9.6 kbps), point-to-multipoint broadcast (one way) data (2.4-9.6 kbps), and various intelligence and special user circuits.

Two NCTAMS and two NCTS are primarily responsible for Naval UHF SATCOM:

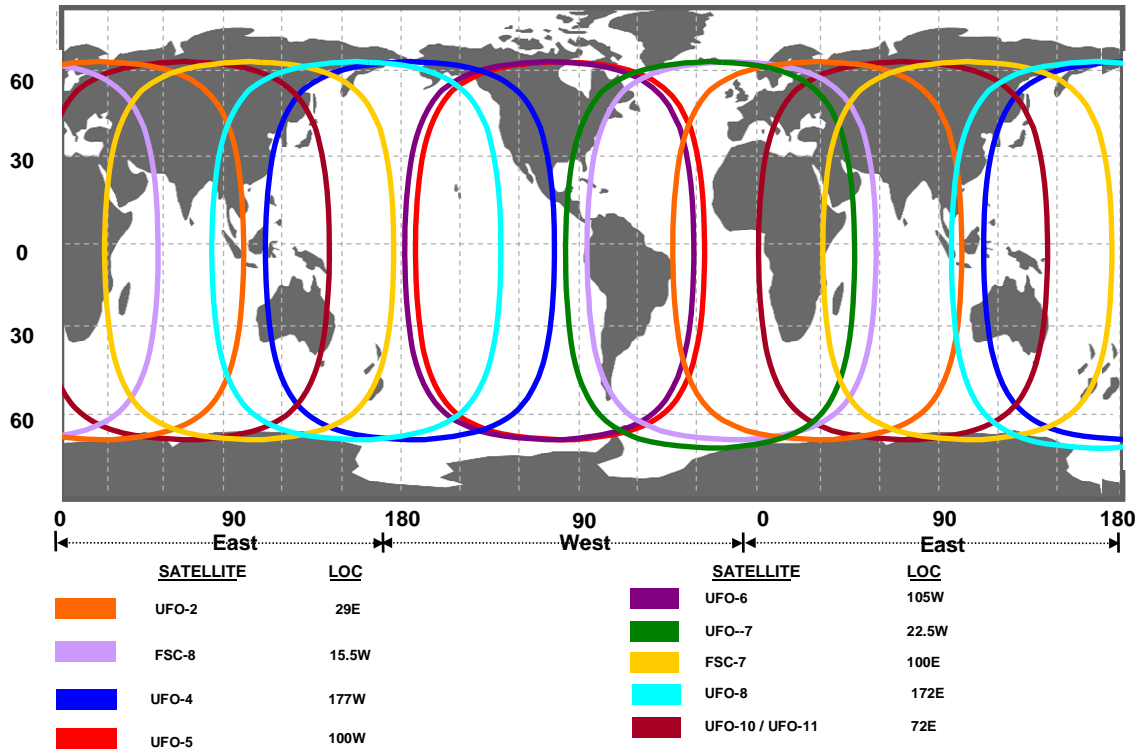
- NCTAMS LANT, Norfolk VA
- NCTS Naples, Italy
- NCTAMS PAC, Wahiawa HI
- NCTS Guam, Finegayan Guam

USJFCOM UHF SAR procedures are available at the Global SATCOM Support Center SIPRNET web page. The current URL is <http://strat.afspc.af.smil.mil/GSSC/default.aspx>:

The UHF satellite constellation and capabilities are depicted in Figure 5-2 and Table 5-1.

UNCLASSIFIED FOR OFFICIAL USE ONLY

# UHF UFO/FSC FOOTPRINTS



UNCLASSIFIED FOR OFFICIAL USE ONLY

**Figure 5-2**  
**UHF Satellite Constellation**

Satellites	Channels		Capabilities
	5-kHz	25-kHz	
UFO-2	21	17	UHF
UFO-4, 5, 6	21	17	UHF, EHF (E) Subsystem (11 Channels)
UFO-7	21	17	UHF, Enhanced EHF (EE) Subsystem (22 Channels)
UFO-8, 10	21	17	UHF, Enhanced EHF, Global Broadcast System (GBS)
UFO-11	25	19	UHF, EE, GBS

**Table 5-1: UFO Capabilities**

### 5.2.3 SUPER-HIGH FREQUENCY (SHF) DEFENSE SATELLITE COMMUNICATIONS SYSTEM (DSCS)

SHF DSCS provides tactical commanders and warfighters seamless and robust access to the DII/DISN for improved C4ISR support as well as enhanced communications interoperability with other U.S. forces operating in a Joint tactical environment.

The SHF SATCOM terminal AN/WSC-6(V)5/7/9 is designed for use on a variety of fleet platforms and provides single or dual channel access to the DSCS and WGS. Single channel access supports plain old telephone system (POTS) and DISN access. The single channel system aboard ship utilizes a dual or single antenna system to provide a clear view of the satellite.

SHF SATCOM interface to shipboard systems is accomplished through the use of various multiplexers and the ADNS. This same infrastructure is provided ashore for interfacing the shore network.

#### **Obtaining SHF Satellite access.**

Processes and Satellite Access Request (SAR) formats are available at the Global SATCOM Support Center (GSSC) and Regional SATCOM Support Center (RSSC) SIPRNET web sites.

GSSC: <http://strat.afspc.af.smil.mil/GSSC/default.aspx>

RSSC CONUS:

<http://strat.afspc.af.smil.mil/GSSC/CONUS/default.aspx>

RSSC PAC : <http://strat.afspc.af.smil.mil/GSSC/PAC/default.aspx>

RSSC EUR : <http://strat.afspc.af.smil.mil/GSSC/EUR/default.aspx>

Particular attention must be paid to lead times for submission of SARs.

All Naval terminals operating on the DSCS satellites are required to submit the 8-hour SHF/C4I report at 0300Z, 1100Z and 1900Z daily to the NCTAMS via Timeplex. The primary NCTAMS will consolidate all 8-hour reports for the perspective satellite and submit as a minimum to the primary and secondary Wideband SATCOM Operations Center (WSOC) no later than 0400Z, 1200Z, and 2000Z daily.

Naval terminal operators must be aware of the importance of the 8-hour SHF/C4I report. It provides trend analysis data for ensuring quality communications, data on the current status of C4I missions, and modeling of SHF/C4I carriers. Ship location is a critical element in determining link and satellite supportability. "Last reported" and "No report received" unacceptable report statuses.

5.2.4 COMMERCIAL WIDEBAND SATCOM PROGRAM (CWSP)

The C-band commercial SATCOM capability provides up to 4.096 Mbps throughput to ships configured with an AN/WSC-8 system and up to 512 Kbps throughput to ships configured with an AN/WSC-6 (v)9 with the MD-1030 or MD-1366 SATCOM modems. As next generation SATCOM Modems are introduced to the fleet and as the shore infrastructure is modernized, higher throughputs may be realized. The current architecture of the Navy's Commercial SATCOM structure may be found at the NETWARCOM Global C4 Readiness website under CWSP link at the following URL:

[http://sgeminii.spawar-chas.navy.mil/c4I\\_DisplaySatellite/DisplaySatellite.aspx?objectId=3314&Title=CWSP&orderby=4&systemName=SATCOM&group=](http://sgeminii.spawar-chas.navy.mil/c4I_DisplaySatellite/DisplaySatellite.aspx?objectId=3314&Title=CWSP&orderby=4&systemName=SATCOM&group=)

SAR/GAR procedures for legacy CWSP and DoD Teleport access can be found in GCIB 7E located on each of the NCTAMS SIPRNET websites.

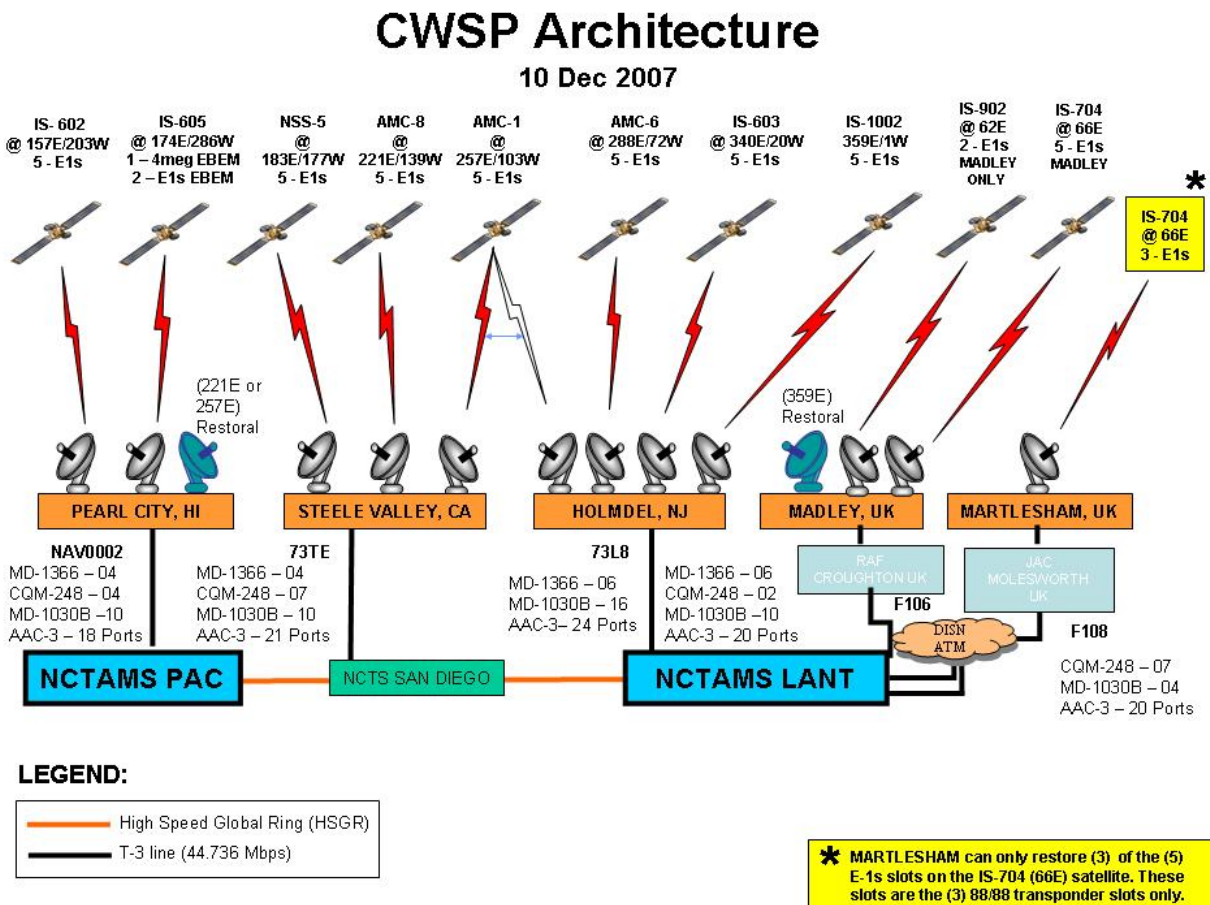
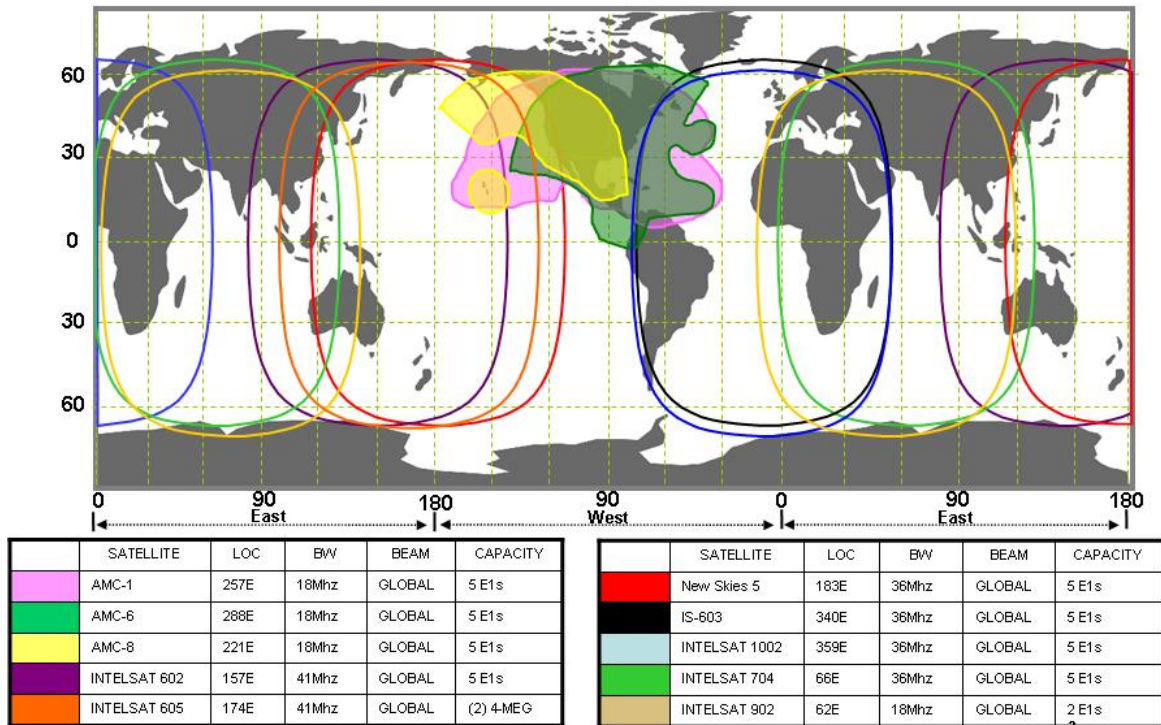


Figure 5-3  
CWSP Architecture



**Figure 5-4  
CWSP Satellite Coverage**

**5.2.5 COMMERCIAL BROADBAND SATELLITE PROGRAM (CBSP)**

CBSP and the Navy Multi-band Terminal (NMT) are the two high data throughput Navy SATCOM programs for wideband SATCOM in the future.

CBSP was approved in March 2007 as a Rapid Deployment Capability (RDC) program. It replaces the Commercial Wideband Satellite Program (CWSP) and International Maritime Satellite (INMARSAT) High Speed Data (HSD) program FY07 to FY13. The current CBSP requirements includes 195 terminals, 118 of which are funded FY08 through FY13. The remaining 77 terminals and any additional requirements (e.g., Command ships, Hospital ships, Submarine Tenders, and Military Sealift Command (MSC) ships, etc.) will be addressed in POM-10 budget process.

The threshold for Unprotected Wideband SATCOM (SHF, EHF, and Commercial) space segment in the Fleet includes:

- 1. Small ships: 0.881 Mbps



2. Unit level ships: 3.6 Mbps

3. Force level ships: 21.4 Mbps

The strategy includes that the Wideband SATCOM space segment thresholds will be achieved with CBSP, EHF SATCOM, SHF SATCOM, GBS, ADNS upgrades and the Enhanced Bandwidth Efficient Modem (EBEM) modem.

The current Navy vision includes MILSATCOM and augmentation with Commercial SATCOM. This includes sustaining CWSP and INMARSAT until the transition to CBSP is complete.

#### **5.2.6 WIDEBAND GLOBAL SATCOM (WGS)**

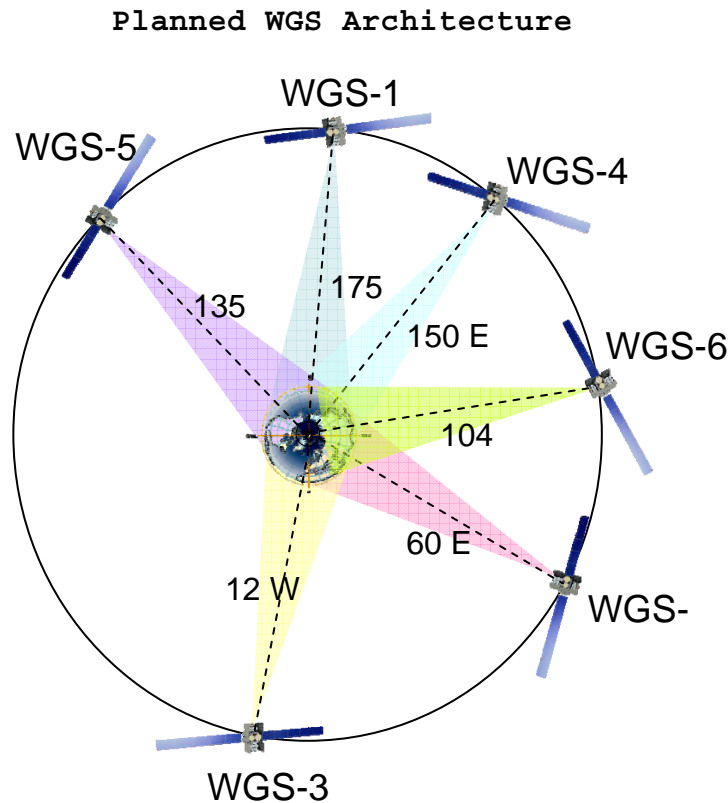
Starting in mid-2010, Wideband Global SATCOM (WGS) satellites will provide DoD wideband (X, Ka/GBS and 2-way Ka) communications coverage supporting tactical and fixed users and eventually replace the coverage currently provided by DSCS and GBS Ka services available via GBS payloads on UFO satellites. WGS satellites will initially complement the DSCS III service life enhancement program (SLEP) and GBS payloads and eventually replace the current DSCS and GBS constellations.

WGS will provide services to the DoD, Australia, and Canada as well as to other Government and Allied users under unstressed conditions. The system will support continuous 24/7 wideband satellite services to tactical users and some fixed infrastructure users. Limited protected services will be provided under conditions of stress to selected users employing terrestrial modems capable of providing protection against jamming.

The combined wideband SATCOM system consists of space vehicles of multiple types, control terminals and facilities, and user terminals. WGS will provide an increase in access and worldwide coverage for both transportable/mobile and fixed users.

The space segment will support communication services by operating in the military X-band frequency and in the WGS broadcast Ka-band frequency similar to the Phase II GBS in service today in order to interoperate with existing and new X-band and GBS terminals. The WGS will also provide a new two-way military Ka-band capability to support the expected military mobile/tactical two-way Ka terminal population with greatly increased system capacity. The satellite payload shall be capable of supporting at least 1.2 Gbps aggregate simplex throughput. Each WGS Satellite will provide bandwidth equal to the total of the existing DSCS constellation. Each satellite orbital configuration will provide services from 65° north latitude to 65° south latitude, and for all longitudes accommodated within the field of view of the satellite. As an objective, the

satellite will provide services to 70° north latitude. X-band services will augment services provided by DSCS III satellites. The Ka-band services will augment broadcast service provided by GBS payloads on UFO satellites and also support two-way network services besides broadcast. Additionally, WGS satellites will support services that require cross-banded connectivity: X-band uplinks to Ka-band downlinks and Ka-band uplinks to X-band downlinks. All WGS satellite configurations will be of a functionally identical design within each orbital position. A total of 6 WGS satellites are planned for launch with WGS-1 already on-orbit in testing (Dec 07) and the launch of the final WGS Satellite (WGS-6) planned for late 2012.



**Figure 5-5  
WGS Coverage**

The WGS satellites will support a variety of network topologies that include broadcast, hub-spoke, netted, and point-to-point connectivity. Limited protection against jamming or interference will, in general, only be possible for those communications networks that employ modems with modulation schemes capable of providing protection against jamming. In certain situations, gain discrimination that may be inherent in the design and emplacement

of the WGS satellite antenna patterns may also provide some measure of protection against jamming and interference sources located at various distances from friendly forces.

The WGS satellites will support Ka-band terminals located in several narrow coverage areas and in at least one expanded narrow coverage area. The WGS satellites will provide two-way and broadcast services within narrow coverage areas to deployed tactical forces in theater as well as to fixed gateways, broadcast injection sites, satellite control sites, and out-of-theater tactical users such as air bases and Naval Strike Groups. The expanded narrow coverage area is several times larger than the narrow coverage area.

### **5.2.7 EXTREMELY HIGH FREQUENCY (EHF) SATELLITE COMMUNICATIONS (SATCOM)**

EHF SATCOM provides Joint interoperable Low Data Rate (LDR) and Medium Data Rate (MDR) Low Probability of Intercept (LPI) / Low Probability of Detection (LPD) and anti-jam communications capability for naval warfighters in submarines, ships, and shore commands.

EHF has a very short wavelength and signals can be affected by rain. EHF SATCOM is generally operated as:

1. Simplex
2. Half Duplex
3. Full Duplex

Simplex is defined as a communications link that operates in one direction only. AM/FM radio, as well as Fleet Broadcast, and Global Broadcast System (GBS) are examples of Simplex communications.

Half Duplex means that the exchange of information can occur in either direction, however, only one can transmit at a time. The best example of Half Duplex communications is on a radio telephone (RT). One station will transmit a message and end the transmission with a proword of *Over* or *Out*, thus notifying other stations that it is OK to transmit.

Full Duplex indicates that communications can occur in both directions, simultaneously between two stations. A standard telephone is an example of Full Duplex communications links.

The effective Concept of Operations (CONOPS) for Naval Communications via the Extremely High Frequency (EHF) Military Satellite Communications (MILSATCOM) System provides amplifying and up-to-date information on the Navy's use of EHF communications systems and services.

The Navy EHF SATCOM Program (NESP) AN/USC-38 Variant (V) terminal is the Navy's segment of the Joint Military Strategic and Tactical Relay (MILSTAR) program. It provides Navy units with networked, point-to-point or broadcast connectivity through:

1. Three UHF Follow-on (UFO)/ "E" (EHF) satellites (UFO/E 4, 5 and 6).
2. Four UFO/EHF Enhanced (EE) satellites (UFO/EE 7, 8, 10 and 11).
3. Three Interim Polar Satellites (IPS).
4. Two Milstar Block I LDR satellites (FLT 1 and 2).
5. Three Milstar Block II MDR satellites (FLT 4, 5 and 6).

Future improvements include Advanced EHF (AEHF) system capable of 75 bits per second (bps) to 8.2 mega bits per second (Mbps) data rates with a total satellite capacity of 400 Mbps, submarine report-back encryption, automated satellite handover, and Enhanced Polar System (EPS).

#### EHF Capability Requirements:

1. Must provide CORE and HARD CORE communications.
2. Must be Anti-Jam.
3. Must be LPI/LPD (available for use during Emission Control (EMCON)).
4. Nuclear event detectable and survivable.
5. LDR (75 - 2400 bps).
6. MDR (4.8 bps - 1.544 Mbps).
7. Capable of netted, broadcast and point-to-point communications (voice, data, TTY and facsimile).
8. Joint interoperable.

#### Space Segment:

There are presently 14 geosynchronous satellites worldwide that support the EHF SATCOM system. In addition to the five Milstar satellites there are seven UFOs (UFO 4, 5, 6, 7, 8, 10 and 11) and two IPS. The third IPS will launch in the near future in support of Polar EHF communication requirements. These satellites have Satellite Resource Controller (SRC) computers onboard that dynamically process the uplink signals from all terminals communicating and produce downlink signals for each beam so every terminal receives the appropriate communication

service. The SRC also furnishes downlink synchronization signals for use by terminals to acquire, logon and track the satellite in time and space.

#### Milstar System Description:

Milstar is a military satellite communications system that provides the Department of Defense and military in the field with reliable, secure, LPI/LPD, anti-jam, and survivable communications between fixed-site, mobile, and portable terminals. Functionally, Milstar consists of three segments: the Space Segment, Mission Control Segment (MCS), and the Terminal Segment.

Milstar Blocks I and II provide world-wide connectivity from 65 degrees South latitude to 65 degrees North latitude using crosslinking capabilities and a variety of antennas and coverage patterns with data rates from 75 bps to 1.544 Mbps.

#### **5.2.7.1 MILSTAR**

The Air Force is designated the System Manager for Milstar and has designated Air Force Space Command (AFSPC) as the Milstar Satellite System Expert (SSE). As SSE, AFSPC controls operations and communications payload management, supports the Milstar program with manpower, equipment, training, and facilities from Space, Air Force 50<sup>th</sup> Space Wing and the 4<sup>th</sup> Satellite Operations Squadron (4SOPS). Facilities include the Milstar Satellite Operations Center (MSOC), the Constellation Control Station (CCSS), the Satellite Operations Center (SOC), and the Milstar Support Facility (MSF).

Together, these Milstar managers are responsible for providing survivable, enduring, minimum essential command and control communications through all levels of conflict for the President of the United States, Secretary of Defense, and warfighting Combatant Commanders (COCOMs) worldwide. MSOC is the Controlling Authority for Milstar Transmission Security (TRANSEC) keys.

#### The Terminal Segment

The AN/USC-38 Variant (V) series LDR/MDR is the Navy's EHF terminal under the Navy EHF Satellite Program (NESP) Program of Record (POR). It is packaged into three equipment groups:

1. High Powered Amplifiers (HPA)
2. Communications Equipment Group (CEG)
3. Antenna Pedestal Group (APG)

Table 5.2 lists all the AN/USC-38 configurations utilized by the U.S. Navy.

Nomenclature	Antenna Size	Abbreviated Name
AN/USC-38 (V) 1	5.5 inch	Sub LDR
AN/USC-38 (V) 2	34.5 inch	Ship LDR
AN/USC-38 (V) 3	6 ft	Shore LDR
AN/USC-38 (V) 4	34.5 inch	Ship LDR/MDR Appliqué
AN/USC-38 (V) 5	54 inch	Ship LDR/MDR Appliqué
AN/USC-38 (V) 6	6 ft	Shore LDR/MDR Appliqué
AN/USC-38 (V) 7	10 ft	Shore LDR/MDR Appliqué
AN/USC-38 (V) 8	5.5 inch	Sub HDR Appliqué
AN/USC-38 (V) 9	54 inch	Ship MDR Follow-on Terminal (FOT)
AN/USC-38 (V) 10	10 ft	Shore MDR FOT
AN/USC-38 (V) 11	5.5 inch and 16.25 inch	SUB HDR FOT
AN/USC-38 (V) 12	16.25 inch	SUB HDR FOT
AN/USC-38 (V) 13	16.25 inch	SUB HDR FOT

**Table 5-2 U.S. Navy EHF Terminals**

### Milstar Satellite Coverage

#### Milstar Block I (LDR)

FLT 1 and 2 satellites have a wide variety of user coverage provided by four EHF LDR antennas:

- a. 1 Earth Coverage (EC) - Tx/Rx
- b. 6 Agile - 5 Uplink (U/L) and 1 Downlink (D/L)
- c. 1 wide steerable spot beam (1.7°) - Tx/Rx
- d. 2 narrow steerable spot beams (1°) - Tx/Rx

Each beam type provides a different coverage "footprint" within the field of view (FOV) of the satellite. EC beams are similar to those on other EHF payloads. Agile beams are different in that they are designated either "uplink" or "downlink", and cannot transmit and receive like other EHF antenna types mentioned previously. One of the six Agile antennas is designated the "Downlink Agile" beam, and the remaining five beams are designated for uplink only. Agile beams cover the same geographic area as the EC antenna; however, not in the conventional sense. The Agile beam coverage is made up of 37 spot beam-like elements creating a honeycomb pattern within the FOV. The Antenna "scans" over the FOV of the satellite, activating each honeycombed cell in succession. Only one of these cells (approx. 1440 nm in diameter at nadir) may be active at any one time per service, thus providing

coverage over the FOV of the satellite, but on a time/location shared basis.

Milstar LDR spot beams are similar to others discussed, except they are narrower. Spot beams A and B are 1° wide (350 nm at nadir) and spot beam C is 1.7° wide (600 nm at nadir).

Milstar I satellites have 144 EHF LDR channels available for user communications services. These channels are distributed among the antennas to promote maximum resource efficiency. Table 5.3 depicts Milstar I LDR channel to beam assignments.

BEAM	COMM CHNLS	BEAM	COMM CHNLS
Earth Coverage	32 channels	High Hop Rate Agile	4 channels
Spot A	16 channels	Low Hop Rate Agile	4 channels
Spot B	16 channels	Reportback Agile	36 channels
Spot C	32 channels	Acquisition Agile	0 channels
Downlink Agile	0 channels	CINC Agile	4 channels

**Table 5-3  
Milstar I LDR Channel-to-Beam Assignments**

**Milstar Block II (LDR/MDR):**

FLT 4, 5 and 6 satellites have all the same LDR and crosslinking features of Block I satellites with an additional MDR payload added to support higher data rate communications. Since Block II satellites have the same LDR payload as Block I satellites, beam coverage options are identical for Milstar II LDR payloads.

The MDR payload has a separate set of eight antennas dedicated to that payload. These antennas are all 1° wide (350 nm at nadir) and capable of simultaneous transmit and receive operation. Two of the eight beams are designated Nulling spot beams (NSBs), and have higher Effective Isotropic Radiated Power (EIRP), therefore provide better downlink margins. NSBs have the capability to detect uplink jammers and will automatically produce nulling patterns within the area of coverage in order to defeat jamming signals. The nulling action effectively creates a hole in the coverage pattern so that energy coming from a terrestrial jammer cannot reach the uplink channel on the payload.

The other six antennas are designated Distributed User Coverage Antennas (DUCAs) and have a 2° downlink beam coverage area approximately 800 miles in diameter. DUCAs have no nulling capability.

When used individually, the area supported by a NSB or DUCA is referred to as a Medium Service Area (MSA). The coverage of two NSBs or DUCAs can be combined to form a Wide Service Area (WSA).

Full Service Area (FSA) coverage, normally provided by an EC beam, is not available on the EHF MDR payload. Users may, however, log onto the satellites' EHF LDR payload via any of its beams and request MDR spot beam repositioning in order to log onto and communicate via the MDR payload.

Milstar II satellites each provide 32 MDR channels distributed among eight MDR antennas. Table 5.4 shows the default channel-to-beam configuration for MDR payloads.

Channel Group A		Channel Group B	
Beam	Channels	Beam	Channels
DUCA A1	4	DUCA B1	4
DUCA A2	1	DUCA B2	1
DUCA A3	1	DUCA B3	1
NSB A	10	NSB B	10

**Table 5-4  
Milstar II MDR Channel-to-Beam Assignments**

EHF MDR protocol supports up to a T-1 data rate (1.544 Mbps). Throughput being a function of gain calculations (primarily determined by antenna dimensions) means not all terminals will be capable of utilizing MDR's maximum potential. What MDR lacks in signal robustness (compared to EHF LDR), it more than makes up for in data rates: 4.8, 9.6, 16, 19.2, 32, 64, 128, 256, 512, 1024, and 1544 kbps, with up to 128+ kbps for protected systems. EHF MDR broadcast service does not include the ability to cross band the fleet broadcast to UHF. Three MILSTAR II satellites (Flights 4, 5, and 6) provide the space segment MDR capability. The current connectivity for large and small deck ships is based on a hub-spoke ADNS architecture, with the hub being at the NOC and the spokes being individual 128 kbps circuits to MDR-equipped platforms. The hub consists of an ADNS router with 12 high-speed serial ports. Although the router supports 12 ports, only enough cryptographic assets are installed to support 10 circuits.

The ADNS connectivity via EHF MDR is installed at four shore sites:

1. NCTAMS LANT
2. NCTAMS PAC
3. NCTAMS EURCENT
4. NCTAMS Bahrain.

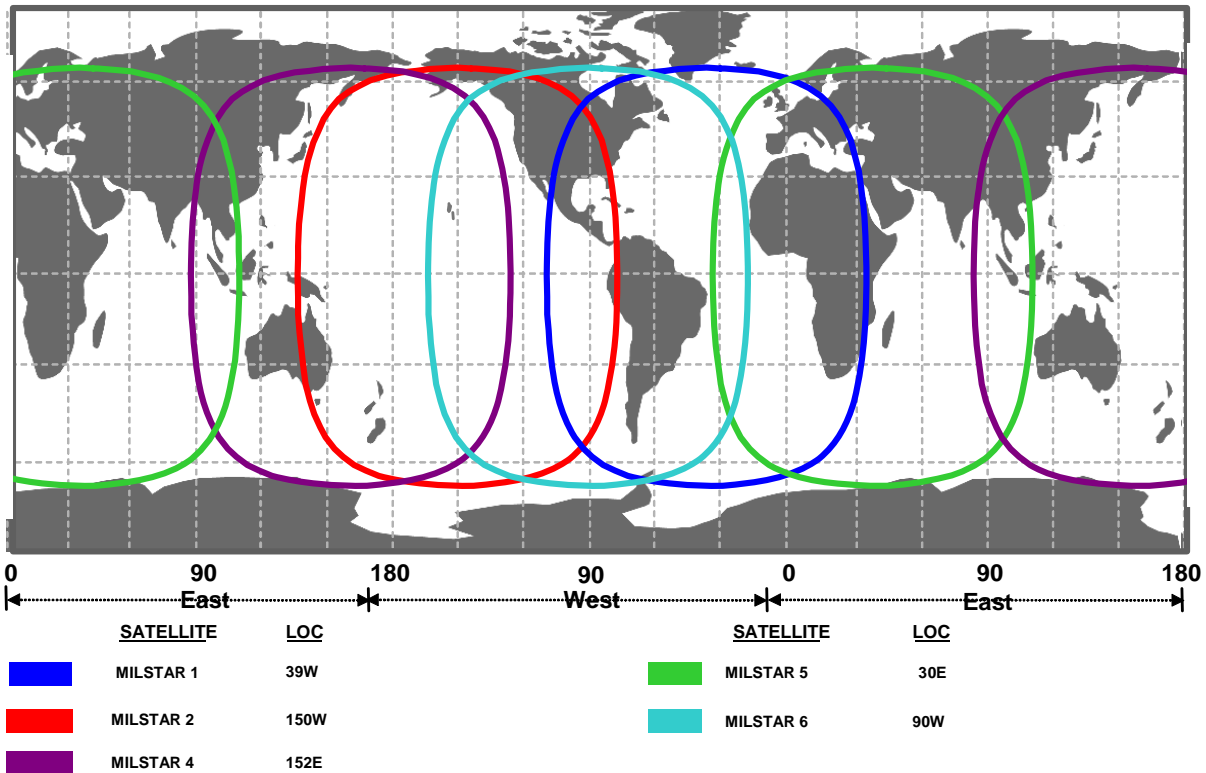
The remaining MDR capacity is used for ship-ship links (e.g., VTC) or Strike Group voice networks (e.g., advanced narrowband digital voice terminal (ANDVT)). EHF MDR is available to all naval command ships including CTF command ships (LCCs and AGFs), SG



command ships (CVs and CVNs), and ESG command ships (LHD, LHA, and soon LPD 17), as well as all TOMAHAWK platforms (DDG and CG).

**UNCLASSIFIED FOR OFFICIAL USE ONLY**

# EHF MILSTAR FOOTPRINTS



**UNCLASSIFIED FOR OFFICIAL USE ONLY**

**Figure 5-6  
MILSTAR EHF Constellation**

UFO/E and UFO/EE:

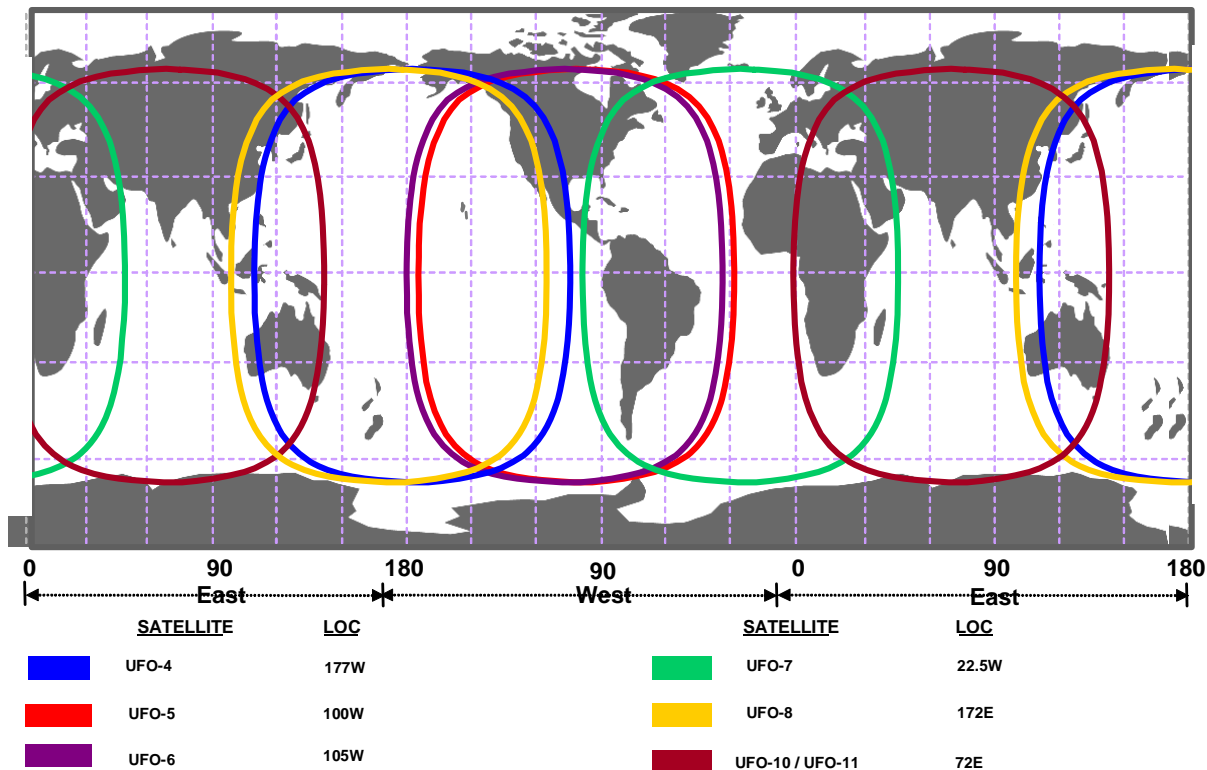
UFO/E and UFO/EE payloads provide one EC and one spot beam antenna, each capable of simultaneous transmission and reception. The EC beam is fixed and useable over the satellite's FOV of the earth, subject to degraded performance at the beam's edge. The spot beam is 5° wide (approx. 1700 nm at nadir) and is steerable over the satellites FOV of the earth.

UFO/E and EE throughput is limited to LDR. The UFO E and EE payloads differ slightly in their respective capacities. UFO/E payloads 4-6 have 11 EHF LDR channels available for communications; seven assigned to the spot beam and four to the

EC beam. This channel configuration cannot be changed nor switched between beams. UFO/EE payloads each have 20 EHF LDR channels available for user communications; sixteen in one group and four in another. These channel groups can be switched between the spot and EC beams in order to meet requirements. That is, 16 channels may be assigned to the spot beam and 4 channels assigned to the EC beam or vice versa. Additional information on UFO/E and UFO/EE operations and communications can be found in the current CONOPS.

**UNCLASSIFIED FOR OFFICIAL USE ONLY**

## EHF UFO/E/EE FOOTPRINTS



**UNCLASSIFIED FOR OFFICIAL USE ONLY**

**Figure 5-7  
UFO EHF Constellation**

### 5.2.7.2 INTERIM POLAR SYSTEM (IPS):

Mobile forces which deploy to the northern latitudes require SATCOM connectivity for command and control among the deployed forces and connectivity with the headquarters elements located in the mid-latitude regions.

The Polar EHF system provides EHF communications supporting mission essential command and control requirements above 65° north latitude. As with other MILSATCOM systems, the Polar EHF system includes the space segment, terminal segment, and control segment.

#### Space Segment:

The polar orbiting satellites and associated EHF communications payloads comprise the space segment for the Polar EHF system. Polar satellites are provided and maintained by a (classified) Host agency of the Federal Government. Each of these satellites circles the earth in an inclined Highly Elliptical Orbit (HEO), commonly referred to as the "Molniya" orbit.

#### Orbital Considerations:

The Molniya orbit is not typical of other EHF satellites which are in geosynchronous orbits over the equator. Geosynchronous satellites have the advantage of being synchronized with the earth's rotation so that they appear as fixed objects in the sky to earth terminals. Therefore, precise terminal tracking is not usually an issue with geosynchronous satellites. A Molniya orbit is quite different, requiring very precise tracking as the satellite rises and sets over the horizon. It is an egg-shaped orbit inclined approximately 63.4° to the equator with a high apogee over the northern hemisphere and a low perigee over the southern hemisphere. Basic characteristics of the Molniya orbit are illustrated in Figure 3-1. Molniya, which means "lightning" in Russian, was the name of the first Russian communications satellites to use it. In this type of orbit, the satellite makes one revolution around the Earth approximately every 12 hours, providing two periods of usable coverage per day. The satellite swings low and fast over the southern hemisphere and then slows as it rises toward its apogee in the northern hemisphere, making it appear to "hover" in the sky over northern territories for long periods of time. This characteristic, in particular, makes the Molniya orbit well suited for communications services in the high-latitude areas.

Polar coverage is defined as the geographic region of the earth above 65° north latitude. Some locations below 65° will have access to Polar EHF payloads for short periods, depending on the specific orbits chosen by the Host satellite provider.

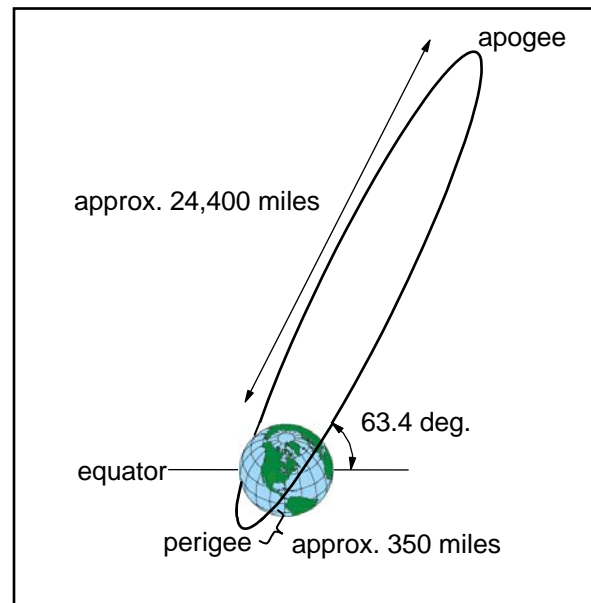
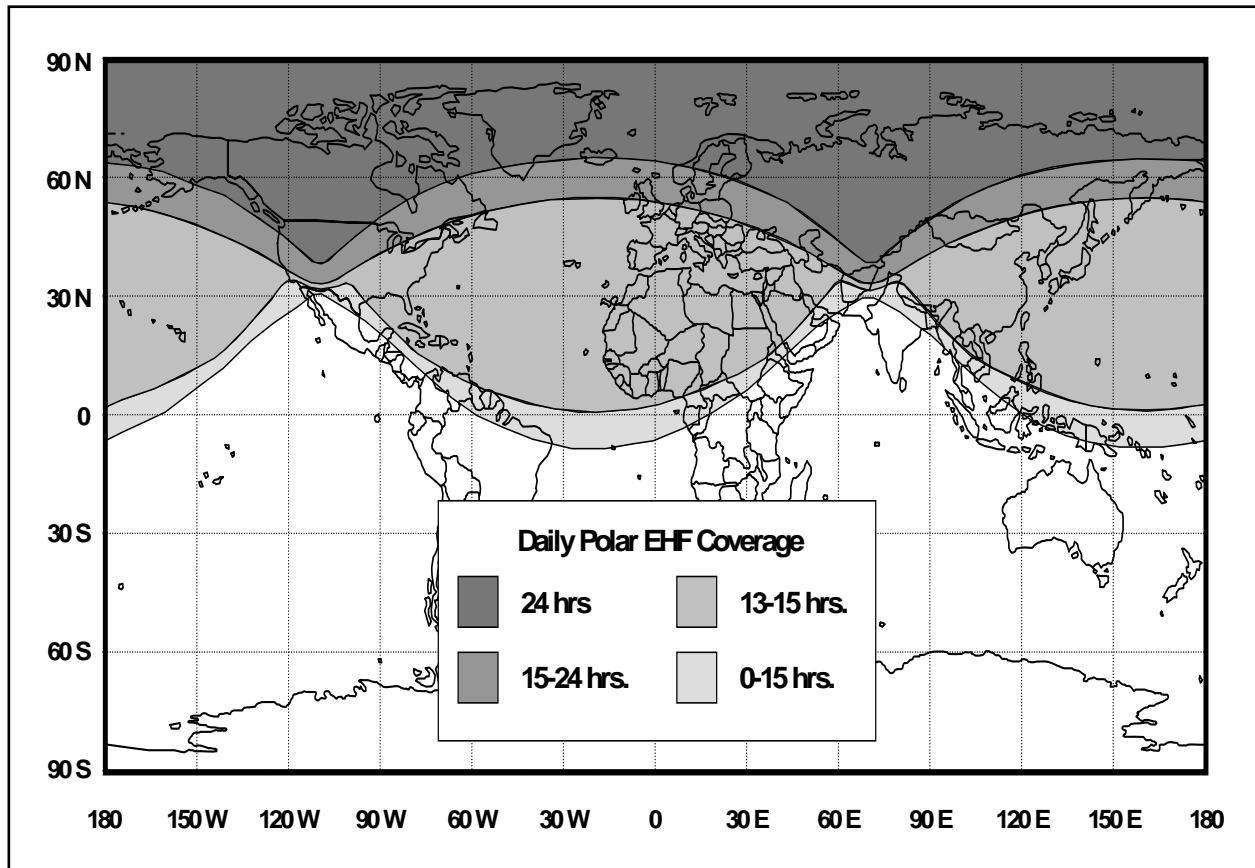


Figure 5-8 shows approximate coverage for the two-satellite constellation. Actual orbital parameters of the host satellites may move this coverage pattern to the left or right.



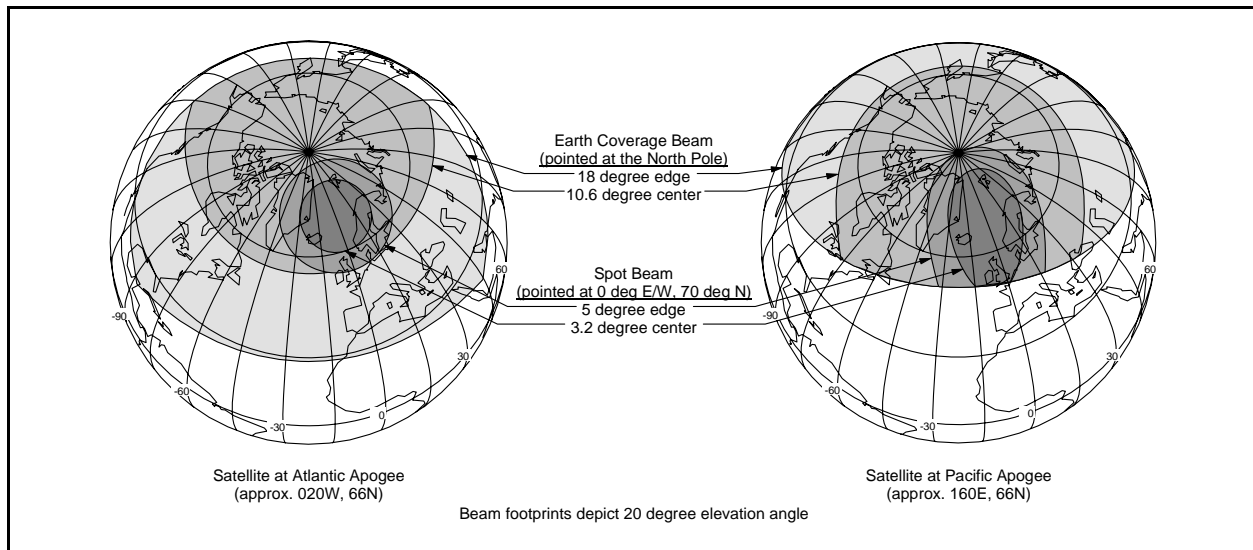
**Figure 5-8**  
**Approximate Polar EHF Coverage (Two Satellites)**

Two Satellite Beams. Two steerable satellite beams are available to support EHF user communications: An 18° steerable earth coverage (EC) beam and a 5° steerable spot beam. The motors used for pointing each beam will be deactivated at the end of each seven-hour operations period. When the payload is reactivated at the beginning of the next operations period, both beams will automatically point to their last commanded position. Figure 5-9 depicts the approximate coverage provided by both beams at satellite apogee (both Atlantic and Pacific apogees shown).

EC Beam. The 18° EC beam covers an area approximately 10,000 miles across. Unlike the EC beams on the equatorial EHF payloads, the EC beam on the Interim Polar system is gimbaled so that it can be steered to a point on the earth's surface by the payload's T&C terminal. As the satellite travels throughout its orbit, the EC beam remains pointed at its designated latitude and

longitude. Terminals within the EC's 10.6° center will have better link margins (both uplink and downlink) than if they were operating on the edge of the beam.

**Spot Beam.** The 5° spot beam covers an area approximately 1,800 miles in diameter and can be repositioned to any point in the field of view on the earth's surface by the user designated as the spot beam controller. As each satellite moves through its orbit, the spot beam will remain pointed at its assigned location. The spot beam provides increased signal gain for both transmit and receive of approximately 6 - 10 dB over that of the EC. Terminals operating in the 3.2° center of the spot beam will receive improved link margins on both the uplink and the downlink with reference to edge of beam operations.



**Figure 5-9**  
**Approximate EC and Spot Beam Coverage**

IPS provides one EC and one 5 degree spot beam, each capable of simultaneous transmission and reception. Additional information on IPS EHF operations and communications services can be found in the current IPS CONOPS.

#### 5.2.7.3 EHF TIME DIVISION MULTIPLE ACCESS (TDMA) INTERFACE (TIP)

Navy TIP is a second-generation controller which offers users a dynamic networking capability over the protected EHF medium. TIP offers protected internet protocol (IP) networking support to the strike groups and ships that do not have IP connectivity via other SATCOM systems. Operating as an ETHERNET "bridge", TIP extends IP Ethernet among TIP sites over EHF Medium Data Rate (MDR), Half-duplex, netted services forming a virtual Local Area Network (LAN).

EHF resources are limited, thus TIP networks make efficient use of these resources. Bandwidth is shared dynamically among all strike group platforms in a netted environment under shared beams. Networks consist of a configuration of subnets and supernets which provide ship-to-ship and ship-to-shore communications thereby giving ships access to shore-based servers.

Each Fleet Commander directs TIP operations within their Area of Responsibility by promulgation of TIP Concept of Operations and/or a Standard Operating Procedure. Specific TIP network configurations are outlined in the Fleet Commander's current or effective EHF Service Plan.

TIP operations for ships and navy shore commands which involve Department of Defense (DOD) teleport sites will be covered by separate instructions.

#### **5.2.7.4 EHF SYSTEMS/SERVICES**

The below systems are used by the Navy and interfaces with the EHF architecture. Specific and detailed information on these systems can be found in the Extremely High Frequency (EHF) Low Data Rate (LDR) and Medium Data Rate (MDR) System User's Handbook, at the Naval Network Warfare Command's website, ([http://sgeminii.spawar-chas.navy.smil.mil/C4I\\_GlobalStatus/GlobalStatus.aspx](http://sgeminii.spawar-chas.navy.smil.mil/C4I_GlobalStatus/GlobalStatus.aspx)).

#### **5.2.7.5 OBTAINING EHF SATELLITE ACCESS**

USJFCOM EHF Satellite Access Request (SAR) procedures are available from the GSSC and RSSC SIPRNET web pages:

The GSSC URL is :

<http://strat.afspc.af.smil.mil/GSSC/default.aspx>.

RSSC CONUS:

<http://strat.afspc.af.smil.mil/GSSC/CONUS/default.aspx>

RSSC PAC : <http://strat.afspc.af.smil.mil/GSSC/PAC/default.aspx>

RSSC EUR : <http://strat.afspc.af.smil.mil/GSSC/EUR/default.aspx>

Particular attention must be paid to lead times for submission of SARs.

#### **5.2.7.6 AFTER ACTION REPORT (AAR)**

USJFCOM will not assign follow on EHF resources for units failing to complete the required AARs following previously assigned missions. All units will notify their appropriate chain of command and the RSSC Conus if they deaccess/end resource usage prior to the mission completion DTG noted in the SAA. The AAR provides sufficient system performance trending. Detailed information should be included to assist EHF managers and users in mission review. Communications planners need to complete the entire AAR with as much pertinent information as possible. Each

communications planner will submit an AAR upon completion of an EHF mission. The AAR will be transmitted via official message traffic. An example of an AAR can be found on the numbered fleet CAS sites.

USJFCOM has a web page for information regarding EHF satellite communications at [www.jfcom.smil.mil/satcomops](http://www.jfcom.smil.mil/satcomops).

#### 5.2.8 MOBILE SUBSCRIBER TO SERVICE (IRIDIUM)

Mobile subscriber service (MSS) systems are satellite-based commercial communications services providing voice and data communications to users equipped with mobile satellite terminals. Common characteristics of MSS systems include coverage of significant portions of the Earth's surface, cellular telephone-like use, connectivity to the Public Switched Telephone network (PSTN) and the Internet. Navy MSS use is currently limited to Iridium. Although authorized, the Navy does not use Inmarsat as an MSS application. Use of other MSS providers requires a waiver from DISA.

The Iridium system is the first commercially available, cross-linked, pole-to-pole global MSS. It is a satellite based, global wireless personal communications network designed to permit any type of narrowband wireless transmission (i.e., voice, data, fax, or paging) to reach its destination nearly anywhere on earth.

The Iridium network consists of a space segment (see Figure 5-10) employing a constellation of 66 satellites in six evenly spaced, nearly polar orbital planes, about 420 nm above the Earth's surface. By linking the satellites and terrestrial gateways, the system provides global access and coverage through specially designed portable and mobile telephones. Seamless connectivity to cellular systems anywhere in the world is provided to phones equipped with an optional cellular cassette. Figure 5-11 depicts the Iridium Ground Segment Architecture.

An Iridium gateway links the orbiting Iridium constellation with the various terrestrial telecommunication systems located within the gateway's territory. It enables subscribers to call and receive calls (unless barred) from non-Iridium telephones throughout the world and provides a "home" where the subscriber's location and calling activity are discretely captured and monitored.

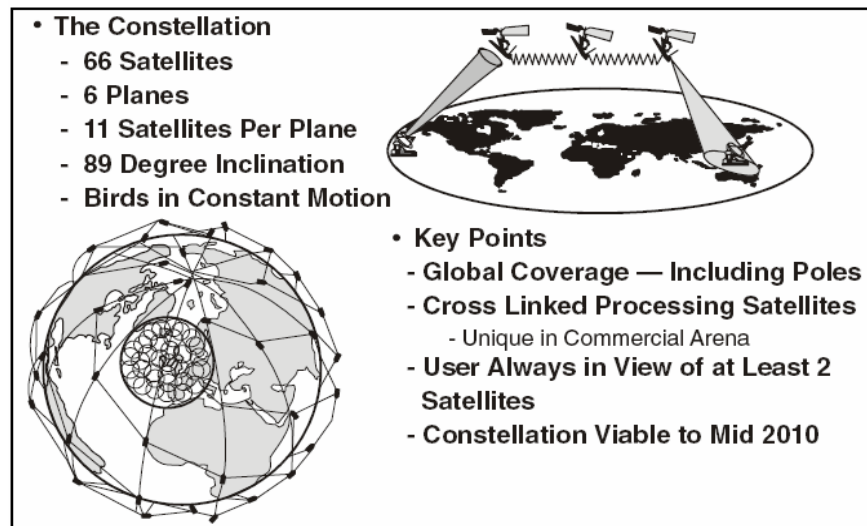
For MSS customers, DoD has established a dedicated Government MSS gateway in Wahiawa, HI for government use through the DISN. Through this gateway EMSS subscribers will have a direct connection into the DISN, which is capable of providing secure services in addition to providing nonsecure access to the PSTN.

The Iridium system is owned and operated by Iridium LLC, a private international consortium of leading telecommunication and industrial companies. Motorola is the exclusive supplier of the

gateways that interconnect the Iridium satellite network with the various terrestrial Public (and private) Switched Telephone Networks (PSTN) and cellular telephone systems throughout the world.

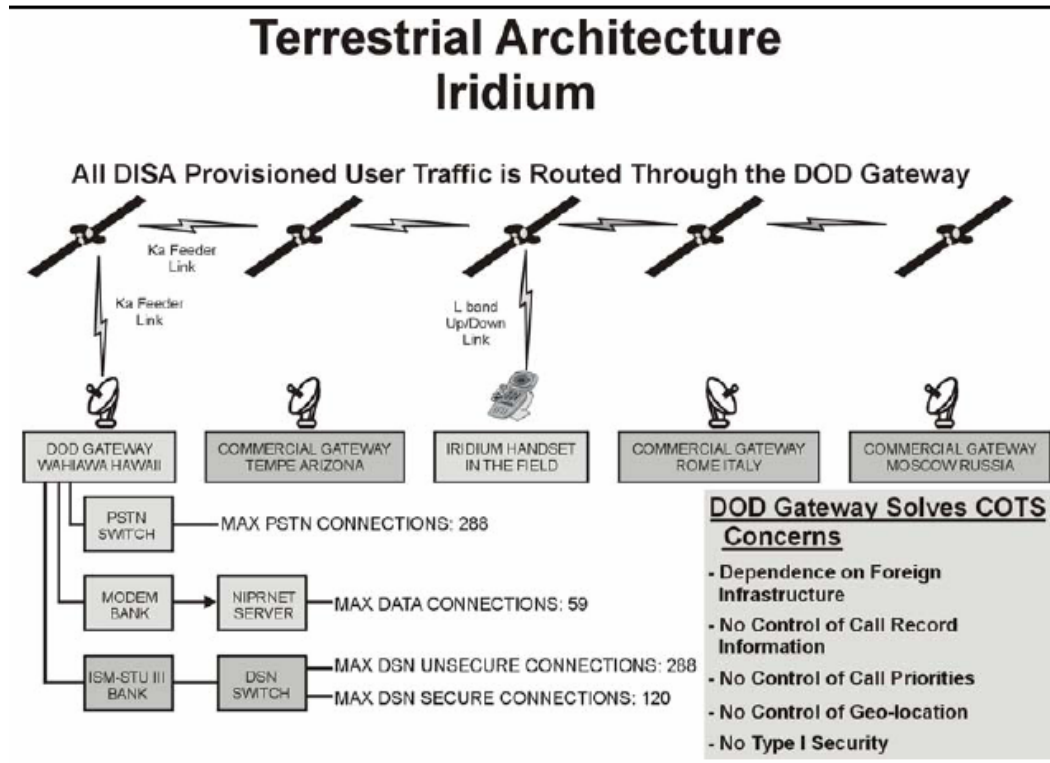
DISA has contracted with Motorola to provide EMSS services to DoD and other federal agencies. Provisioning EMSS equipment and services will be accomplished through DOD's process for procuring telecommunications services and is managed by the Defense Information Technology Contracting Organization (DITCO). The requester is responsible for completing the approval actions as specified in the Service/agency EMSS approval procedures. Iridium provides:

1. One full duplex channel capability for small platforms, subs, mobile, littoral, or shore/beach units secure or unsecure voice.
2. Unsecure data/Internet up to 10 kbps.
3. True global coverage (90° N to 90° S).
4. Small battery-operated handheld terminals and shoebox-sized shipboard terminals.
5. 8-inch omni-directional antenna.
6. L-band.
7. Secure capable system.
8. NSA certified type 1 crypto module.
9. Data capable 2.4 Kbps ISP dial-up or up to 10 kbps direct Internet connection.



**Figure 5-10**  
**Iridium Space Segment**





**Figure 5-11**  
**Iridium ground architecture**

### 5.2.9 INMARSAT HIGH SPEED DATA

The Inmarsat HSD system continues to be a critical communications path for SIPRNET, NIPRNET, and telephone ship-to-shore access for all Navy ships less the CV/CVN/LHA/LHD/AGF and LCC classes. This multipurpose SATCOM system provides both simultaneous voice and IP data up to 128 Kbps. By providing access to the DoD unclassified and classified IP networks, all ships of a Strike Group become participants in a WAN that enables real-time collaborative planning and significantly improved unit SA and group C2. In addition, it supports quality of life communications supporting voice and e-mail exchange between Sailors at sea and friends and family ashore.

The Inmarsat program augments MILSATCOM systems to provide added capacity for fleet voice and data services. The program provides for leases of commercial Inmarsat satellite channels and procurement and fielding of Inmarsat terminals and ancillary equipment to enhance the leased service. In addition, the program accommodates the lease of necessary terrestrial connectivity between Navy hubs (NCTAMS, NCTS San Diego, NCTS Bahrain) and the commercial Stratos Mobile Networks-owned Earth terminals in Canada, the Netherlands, and New Zealand.

The Inmarsat terminals operate in the UHF L-band via the geostationary Inmarsat satellite constellation, enabling point-to-point voice, facsimile, and data. The Inmarsat-B terminal is

based on digital technology and provides digital voice at 16 Kbps, data and facsimile up to 9.6 kbps. The Navy's primary fleet implementation of Inmarsat utilizes a built-in digital modem with capability up to 128 Kbps.

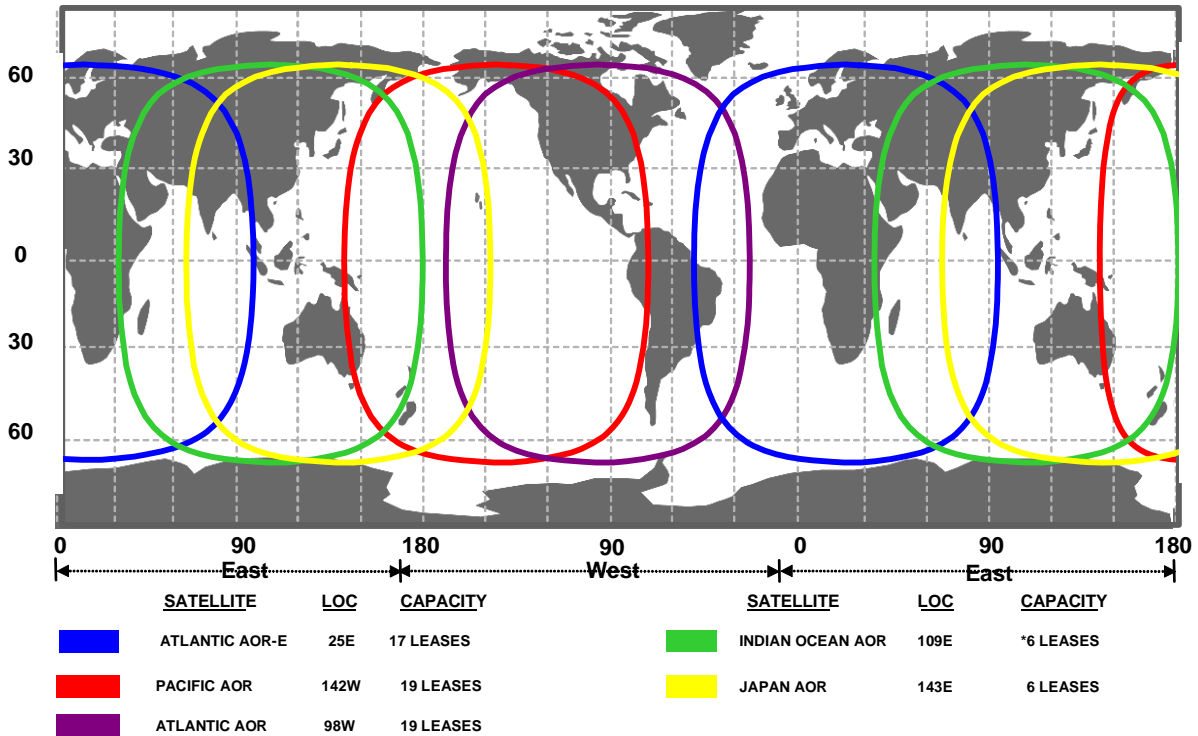
As part of IT-21 requirements, Inmarsat-B HSD multiplexers (AN/FCC-100(V)9s) have been procured and installed in conjunction with leasing dedicated full-time 128kbps channels. Multiplexers and other equipment have also been installed at the Navy hubs to support Inmarsat HSD. The multiplexers are reconfigurable and support variable voice/data rates up to 128 Kbps aggregate, including voice (nominally 3 official lines and one for unofficial Navy Exchange Command (NEXCOM)-supported afloat personal telephone service (APTS), and a data link for NIPRNET, SIPRNET, and JWICS at a nominal data rate of 32 Kbps). A summary of Inmarsat capabilities include:

1. Worldwide coverage (as shown in Figure 5-12)
2. Narrowband point-to-point voice, fax, and data
3. Inmarsat-B HSD single system = 64 Kbps; enhanced system = 128 Kbps
4. SIPRNET, NIPRNET, and JWICS - 32 Kbps
5. Voice channels (dial tones are at San Diego, Norfolk, and Hawaii)
6. Three official lines: 9.6 Kbps STU III, 9.6 Kbps, and 4.8 Kbps
7. NEXCOM APTS: 4.8 Kbps

Note: The Enhanced systems are capable of full 128 Kbps operation or drop down to 64 Kbps.

Procedures for requesting INMARSAT access can be found in GCIB 9A, located on each of the NCTAMS SIPRNET web sites.

# INMARSAT SATELLITE FOOTPRINTS



\*67 Worldwide Lease Channels 01 Jan – 31 Dec 07 (including 1 FMS channel on 109E)

Figure 5-12  
INMARSAT Constellation

## 5.2.10 GLOBAL BROADCAST SYSTEM (GBS)

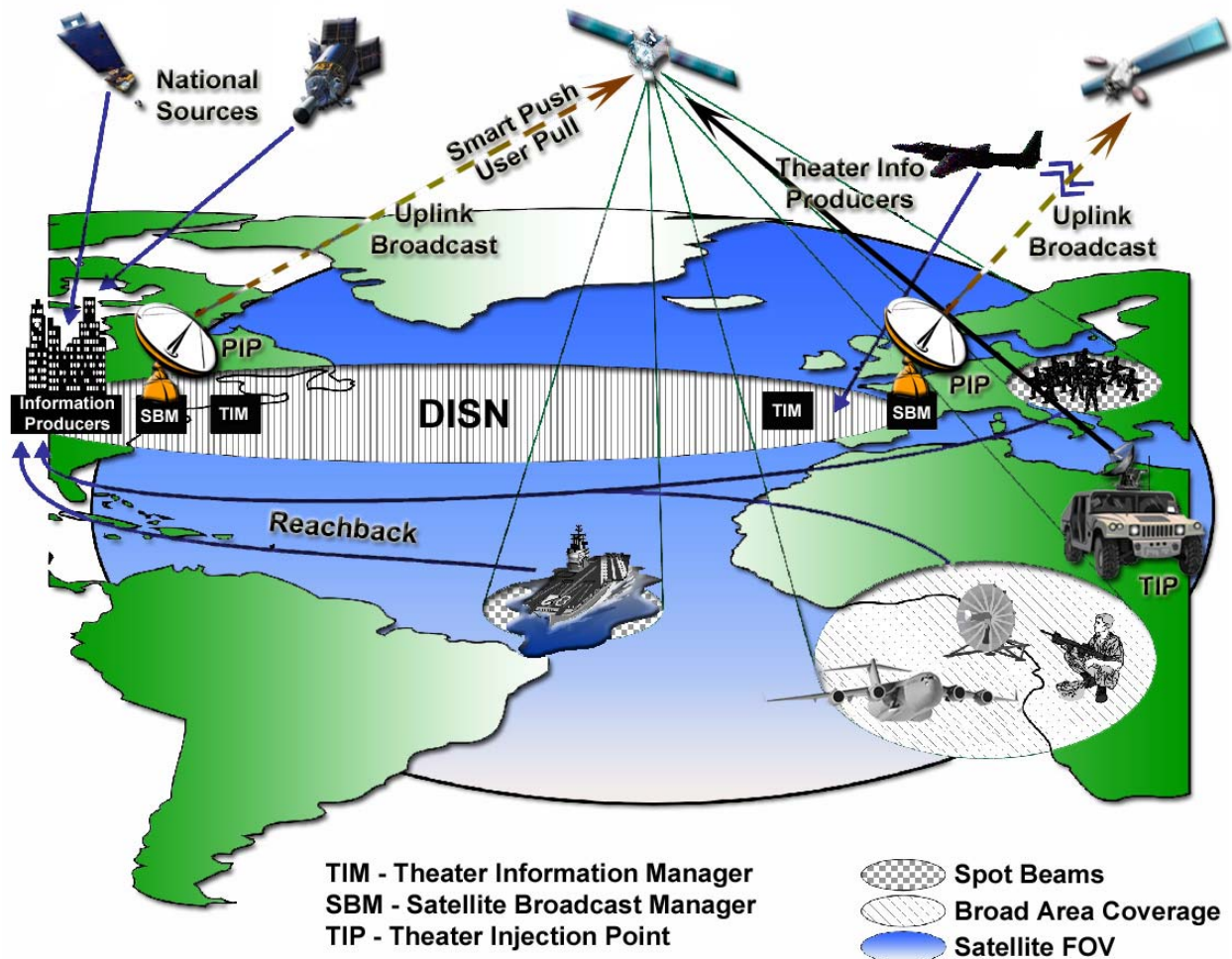
**Overview.** GBS is primarily a broadcast service that augments and interfaces with other communications systems. GBS supports wartime engagements, training and military exercises, special activities, crisis operations, battlefield awareness, weapons targeting, and Intelligence, Surveillance, Reconnaissance (ISR) requirements. GBS provides Joint operations with high-speed, multimedia communications, and information for deployed, on the move (in-transit), and garrisoned forces. Homeland defensive operations are supported via CONUS coverage, which also provides pre-deployment training and exercise support. GBS also supports military operations with United States (US) Allies and Coalition forces dependent on security and cryptographic releasability restrictions.

High-data-rate satellite terminals are characteristically large and fixed, but GBS receive terminals are small, mobile, and receive high-volume data using 1-meter or smaller antennas.

Mobile force elements, free from restrictive large fixed terminals, can receive information formerly available only to command centers. Current GBS technology can support data rates between 1.544 Mbps and 45 Msbps (Mega-symbols per second) depending on satellite capability, but can transmit at lower data rates to support disadvantaged users or to compensate for environmental conditions. Each satellite that supports GBS will be serviced by an SBM and PIP or a TIP. GBS relies on DISN transport capabilities to relay information from national and theater information sources to the SBM for broadcast injection via a PIP. In order to access WGS satellites, the plan is for GBS SBMs to integrate with the DOD Gateways. The Gateway will provide digital video broadcast (standard) technology via the current force Digital Video Broadcasting over Satellite (DVB-S) IP MODEM and the Joint IP MODEM hub supporting deployed users with GBS RS's and transmit-receive VSAT suites. This integration will provide complementary access to tailored information content via UFO/G, WGS, and commercial augmentation satellites. Since GBS enables the storage, retrieval, and dissemination of large information files that could quickly exceed the capability of most mobile users, the tailoring of the "Smart Push" and "User Pull" dissemination architecture for GBS is a significant challenge. This capability is being addressed through several initiatives such as the Information Dissemination Program within the DoD Net Centric Enterprise Services (NCES) Program.

A fundamental feature of GBS is the BMS. The BMS retrieves, accepts, coordinates, and (if required) packages information such as general broadcast products, "Smart Push" products, and "User Pull" products. The required information is gathered from both national and theater sources for broadcast based on the direction and priorities identified by their respective COCOMs and their functional users. The BMS also performs any additional functions necessary to support the efficient use of GBS. These functions include, but are not limited to managing space segment coverage and capacity sharing, providing interface protocols and standards designed to allow information providers to submit information in a form acceptable by the GBS broadcasts, and coordinating with the COCOM TIM cells to apply COCOM's priorities.

Figure 5-13 illustrates a conceptual GBS architecture. The major operational elements of the GBS architecture are: users, information providers, TIMs, SBMs, PIPs, TIPs, RS's, and satellites. Conceptually, the architecture is the same using UFO/G satellites, WGS satellites, or commercial augmentation satellites.



**Figure 5-13**  
**Conceptual GBS Architecture**

The Pacific GBS SIPRNET site (<https://info.gbs-pacom.navy.smil.mil/>) provides guidance and information for users in the PACOM region.

The Atlantic GBS SIPRNET site ([http://207.85.158.53/ip\\_rbm.htm](http://207.85.158.53/ip_rbm.htm)) provides guidance and information for users in the Atlantic Region.

The GBS system is broken down into three physical entities: Transmit Suites (TS), Receive Suites (RS), and Satellites. The TS includes a Satellite Broadcast Manager (SBM) and an Injection Terminal. The Fixed Transmit Suite is an SBM and one or more Primary Injection Points (PIP)s (either collocated or remote), and may include an Extremely High Frequency (EHF) Follow-on-Terminal (FOT). The Theater Injection Point (TIP) includes a Transportable Theater Injection (TTI) and a Theater Satellite Broadcast Manager (TSBM). An RS includes a Receive Terminal (RT)

(any type) and a Receive Broadcast Manager (RBM). These physical entities are comprised of the following three functional segments: The Broadcast Management Segment, the Terminal Segment, and the Space Segment.

The Broadcast Management Segment consists of the following elements: SBM, Theater Satellite Broadcast Manager (TSBM), and the RBM. The Terminal Segment consists of the following elements: PIP, the TTI, the Fixed Ground Receive Terminal (FGRT), the Transportable Ground Receive Terminal (TGRT), the Shipboard Receive Terminal (SRT), the Sub Surface Receive Terminal (SSRT), the Airborne Receive Terminal (ART), and the Manpack Receive Terminal (MRT). The Space Segment consists of the following elements: four UHF Follow On (UFO) transponders per UFO/GBS satellite (UFO 8, & 10), leased commercial transponders and four equivalent GBS "transponders" on the three Wideband Gapfiller satellites. The SBM/TSBM function will build the broadcast data streams, manage the information flow to the appropriate injection point(s) and modulate the uplink carrier for transmission to the satellite(s). Together the SBM/TSBM and PIP/TTI make up a TS/TIP. The RBM functions are to accept and demodulate the downlink signal from the Receive Terminal and support the dissemination of information to the end users. Together the RBM and RT make up an RS. The transmit segment of the GBS system includes both fixed and transportable uplinks. The fixed version of this segment PIP provides the collection of data from the DISN, scheduling of the broadcasts, and transmitting of the broadcasts to the space segment. The transportable version of the transmit segment (transportable injection point) will provide theater commanders the capability to transmit theater information directly to forward users or rear areas to augment the information in the PIP broadcast. The transmit segment will be fitted with equipment to support multiple frequency bands allowing operation with both military and commercial satellites.

GBS supports the National Military Strategy (NMS), including operations with Allies or Coalition forces. In support of NMS, using UFO/G and WGS satellites, GBS provides coverage between 65° North latitude to 65° South latitude. GBS is not designated as a protected system (per Advanced MILSATCOM Capstone Requirements Document [CRD] dated April 1998). If the users require protected or anti-jam communications, then they should seek other media methods and should only use GBS as a secondary delivery means.

GBS provides broadcast services to selected echelons through a layered or scaleable architecture. This architecture compensates for differences in security classification levels, classes of users, and the ways in which users receive information products. Depending on the needs, RS equipment supports a variety of user configurations ranging from stand-alone operations to network integration. Figure 5-14, provides the high-level operational concept for GBS. The numbers in the diagram indicate activities required between various elements that make up the GBS system.

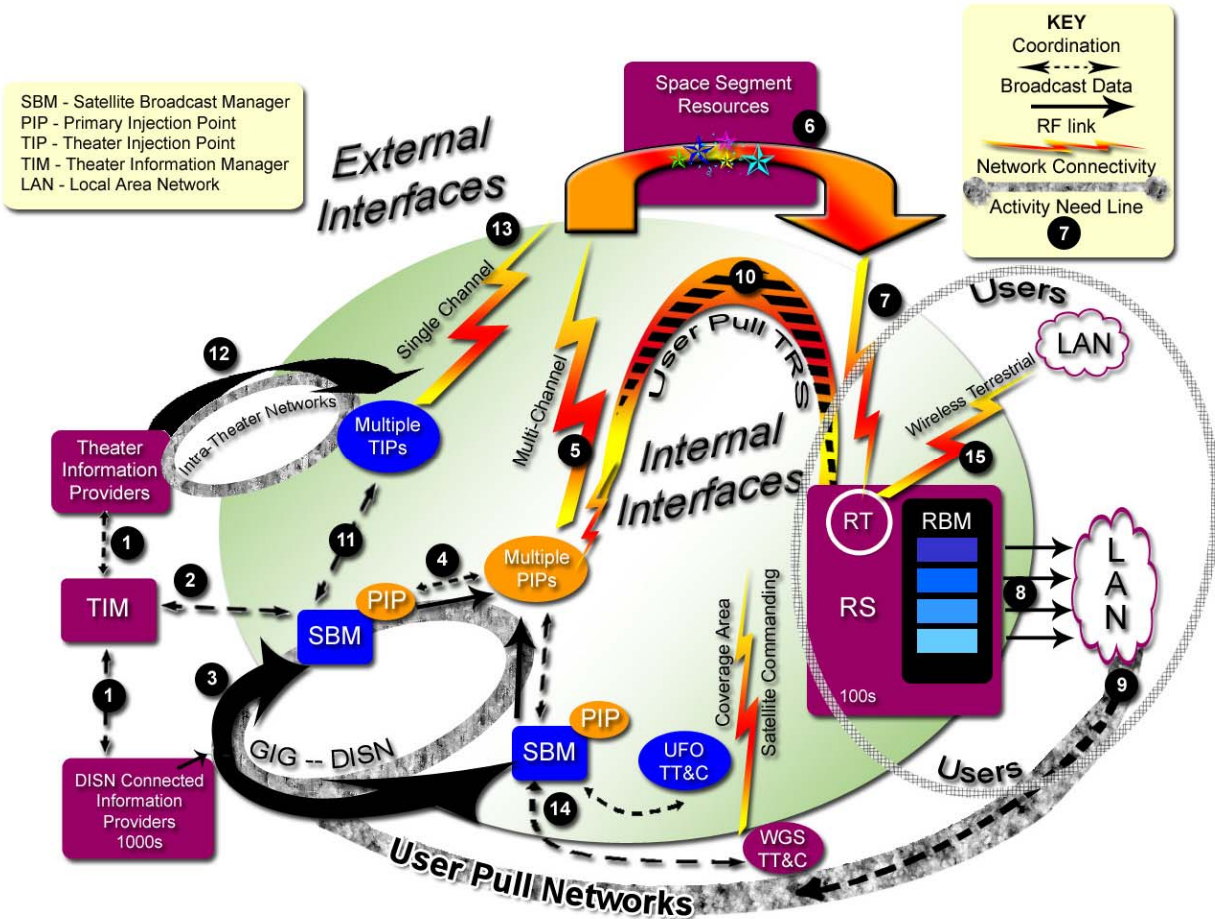


Figure 5-14

**GBS Concept of Operations Overview**

TIMs determine and prioritize candidate broadcast content and coordinate with information providers.

Each TIM documents its information requirements and priorities in databases managed by the BMS, represented here by the SBM. This deliberate planning process identifies all "Smart Push" products, authorizes "User Pull" criteria, and is the basis for beam planning.

Information intended for broadcast is transferred to content storing at the SBM where information is broadcast based upon priorities and beam coverage.

The SBM builds unique broadcast streams for current satellite coverage areas and delivers broadcast streams directly to a PIP.

PIP converts one or more broadcast streams into separate RF broadcast injection signals to the satellites that are supporting

GBS operations.

The satellite receives and amplifies the uplink signal and retransmits to a designated downlink coverage area for one or multiple users.

Each RS processes the satellite's downlink. RF signal and the RBM determine which information products are for its assigned or supported users and separate the information products into different security enclaves and media types.

RS's deliver the broadcast information through various physically separated security enclaves to attached LANs, where the information is made useful by end-user applications.

Users must use existing connectivity capabilities in order to identify specific ad-hoc information needs for inclusion in the broadcast as "User Pull." These requests may go either directly to information providers for direct satisfaction or to the TIM for approval and then to the SBM for GBS-managed inclusion. "User Pull" responses are either single user or COI broadcasts to multiple users.

Alternatively, specially equipped RS's lacking other means for "User Pull" connectivity may use a satellite return channel to initiate "User Pull" requests.

When a TIP is deployed, some coordination is required between the TIP and the SBM, such as transponder allocation times and beam locations. Otherwise, TIP operations are autonomous and independent of the SBM.

The TIP accepts information content from theater information sources when it is operationally more effective or efficient for direct broadcast rather than back-hauling from a SBM.

The TIP uses a Transportable Satellite Broadcast Manager (TSBM) to manage generation of broadcast streams. The current TIP implementation uses a Phoenix SATCOM terminal, previously recognized as the Tactical Theater Injector (TTI), to inject and convert the broadcast stream for RF transmission to corresponding space segment resources (transponders).

The SBM determines how best to execute TIM dissemination priorities and changes in the space segment coverage areas; the SBM directs automated beam movement commands and restores broadcast service after the new coverage is achieved. There are two SBM capabilities that support these functions. The first is direct command execution capability through SBM -dedicated



extremely high frequency (EHF) terminals for Telemetry, Tracking, and Commanding (TT&C) with the UFO/G payloads. The second is a direct path to the Gapfiller Satellite Configuration Control Element (GSCCE) located in Wideband SATCOM Operations Centers (WSOCs) through the Objective Defense Satellite Communications System (DSCS) Operations Control System Network (ODOCSnet) for managing WGS space segment resources and coverage areas that have been dedicated to GBS SBM management. The SBM will not have direct command execution capability of WGS for shared WGS space segment resources. Additionally, the current plan is to use the Common Network Planning Software (CNPS) for WGS GBS planning and resource allocation.

Specially equipped RS's may extend GBS delivery services across wireless networks to user LANs.

The GBS IP architecture uses various types of implemented broadcast services. These services provide the user with different methods to receive products over GBS. The different services are implemented through a spiral development approach with additional capabilities added during each spiral. The five most common types of services are: (1) Streaming Packet (with or without source encryption); (2) IP-to-IP Video; (3) Immediate File Delivery (IFD) (with or without metadata); (4) Mirrored Services (SBM mirrored, source mirrored, or web mirrored); and (5) Power Publisher;

1. Streaming Packet. IP packet streams are source encrypted through the SBM. These packets require no visibility and no intervention by the SBM. There are two options for this service: Streaming Packet and Source Encrypted.

- a. The Streaming Packet option allows any IP stream to be sent to GBS users; this includes files, video, multicast, and pre-encrypted streams.
- b. The Source Encrypted option allows additional classification levels to be supported using source-hosted cryptographic devices. Except under special circumstances, source encrypted information providers are expected to use interoperable cryptographic devices with that of the GBS RS's. The broadcast of compartmented or above US SECRET releasable information may use Keying Material (KEYMAT) management and information-source encryption to restrict access. Compartmented information providers (including Top Secret [TS] Collateral, TS/Sensitive Compartmented Information (SCI), and Coalition or Allied and non-DoD releasable information) intending to use GBS must manage content, priorities, and provide source encryption of their information external to GBS broadcast centers. These information providers shall also use GBS prescribed and interoperable encryption

and communications protocol standards which are integrated with and tunneled through the broadcast.

2. IP-to-IP Video. In this service, multicast video streams are received by the SBM and may be transcoded (converted to a lower data rate) before being broadcasted over the GBS system. This process also allows for broadcasting video with forward error correction (FEC). The FEC supports recovery of lost streaming packets at the RBM.

3. Immediate File Delivery. IFD allows the creation of unique folders at the SBM associated with a COI. When products are delivered to the folder these data files are queued up for broadcast using a "stored and forward" methodology based on available or planned spot beam coverage. Files are pushed from the source over the DISN to the SBM or over tactical communications to the TSBM. The files within the folder are then queued and broadcasted based on their relative content priority and available satellite resources. If the user is not within satellite coverage when the product is delivered to the SBM and the product is retained for future broadcast when the user is under coverage. IFD programs can be paused during transmission if another product (IFD or other delivery service) with a higher mission precedence or content priority is activated. Upon the completion of the transmission of the prioritized product, the IFD resumes transmission until finished. IFD folders have a product time-to-live, when exceeded the content is considered stale and will not be broadcasted.

The IFD with metadata is an enhanced IFD service that allows information providers or broadcast managers to monitor or manipulate the progress of products in their assigned IFD folder's queue. Inquiries and commands permit estimating when a product will be broadcast, changing the content priority ordering of products in the queue, removing products from the queue, pausing the queue, determining which users have satellite coverage, and determining when a specific product was broadcast, but does not report if actually received.

4. Mirrored Services. This service gives information providers the capability to perform information push of their products to a folder at the SBM or TSBM. SBM mirrored services provide the means for the SBM folder's contents to mirror the contents of the information source's folder files. As files are added or modified in the mirrored folder at the SBM, the file is immediately queued for broadcast. Before being broadcasted, the individual files are packaged together rather than sent as a large number of individual files. The entire folder is rebroadcast when the "full-stale-after" time has expired as recorded for each RBM. This full rebroadcast ensures automatic cleanup of the mirror folder for each RBM and allows the RBM to eliminate deleted files or correct otherwise unknown damaged mirror content. All files are rebroadcast after each beam dwell. If a file is deleted at the SBM, the file is also deleted at the

RBM. Each individual RBM is tracked for differences in their mirror based on available satellite coverage during packaging and broadcast opportunities. The objective is for the SBM's folder structure and content to be mirrored in the RBM's folder.

Source mirrored services are similar to mirrored services except the source mirrored service allows the source to identify a directory folder located on a source machine as the home of the program content instead of a directory located at an SBM. However, only "full-stale-after" broadcasts are accomplished; individual RBMs are not tracked for differences in their mirror, and incremental mirror updates are not supported. When the "full-stale-after" clock expires the entire content of the mirror source is brought to and held at the SBM for packaging and broadcast as assigned user RBMs obtain satellite coverage.

Web mirrored services provide the means for website data to be collected by the SBM who creates an internally linked web package according to the crawl configuration parameters set up for the program. The crawled files are made available to the end user through a web browser interface. The crawl is a fully automated, multi-threaded, file-retrieving web spider. Tools assist in setting up the crawl configuration parameters by interactively downloading a website, creating a mirror of the download, searching the site for files of a certain type, and then downloading a list of selected files and their Uniform Resource Locator (URL). Once packaged for broadcast, the product is queued and paused until designated RBMs, which receive the web package, are available under satellite coverage. After each "full-stale-after" has expired, a refresh occurs for the web crawl, package, and queue for broadcast.

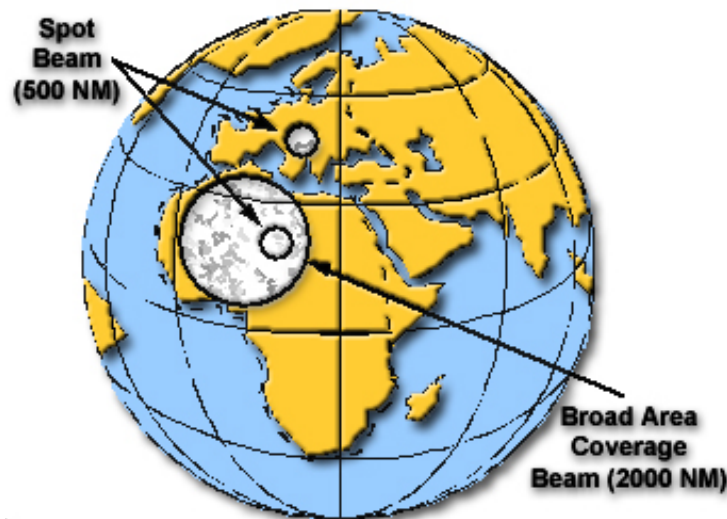
5. Power Publisher. This is a Transmission Control Protocol (TCP) tunnel channel that provides greater control of source content broadcasts. Registered products at the SBM or TSBM set start and stop times and guarantee minimum bandwidth usage of the channel. The information provider can send IP streams and files. The data packets are passed directly onto the broadcast to associate RBMs with satellite coverage, thus avoiding the latency associated with saving files to an IFD folder. Unlike IFD, this service does not use store-and-forward. Products are FEC encoded at the source. Separate Power Publisher services must be registered for each information provider on each transponder used. The product performing this function must be certified in accordance with National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 and other applicable IA policies.

Injection points uplink the broadcast stream to the satellite and must be located within the satellite's FOV. GBS allows for two types of injection points: primary and theater. PIPs will be tied to their respective SBM through appropriately sized communications connectivity. This communications connectivity

should meet the anticipated throughput requirements of the GBS Phase 2 space segment (i.e., up to 4 transponders times 29.5 Mbps [24 Mbps] per transponder for UFO/G and 4 regional broadcasts times 45 Megasymbols per second [MSPS] plus at least 2 theater broadcasts [for TIP broadcast support] times 20 MSPS per WGS satellite). The PIP is the preferred method of injecting broadcast streams. Theater-produced information should be transmitted by available means to the SBM for broadcast via the PIP, whenever possible. This creates a "virtual injection" from theater.

The WGS system will enhance the overall GBS capacity and coverage. For initial operations on WGS satellites, the SBM will integrate with the WGS system by treating each WGS satellite payload as if it were another UFO/G package in planning the broadcasts. WGS satellite capacity will be shared among two-way and broadcast users based on the validated requirements of the supported COCOM/Service/Agency (CC/S/A).

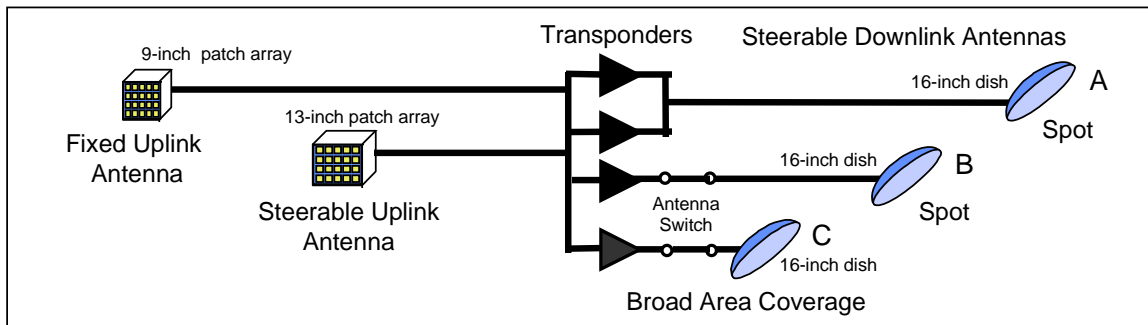
Using the UFO/G satellites, two distinctive broadcast patterns will provide coverage for a specific AOR. A broad area coverage beam covers a large portion (approximately 2000 nautical miles [nm]) of the AOR. A spot beam (also referred to as the Narrow Beam [NB]) covers a smaller, more concentrated area (approximately 500 nm). Figure 5-15 is a scaled depiction of these coverage patterns.



**Figure 5-15**  
**Sample/Generic UFO/G Beam Coverage**

UFO/G satellites have a GBS payload consisting of four transponders, two uplink antennas (one fixed, pointed at the PIP, and one steerable), and three steerable downlink antennas (two

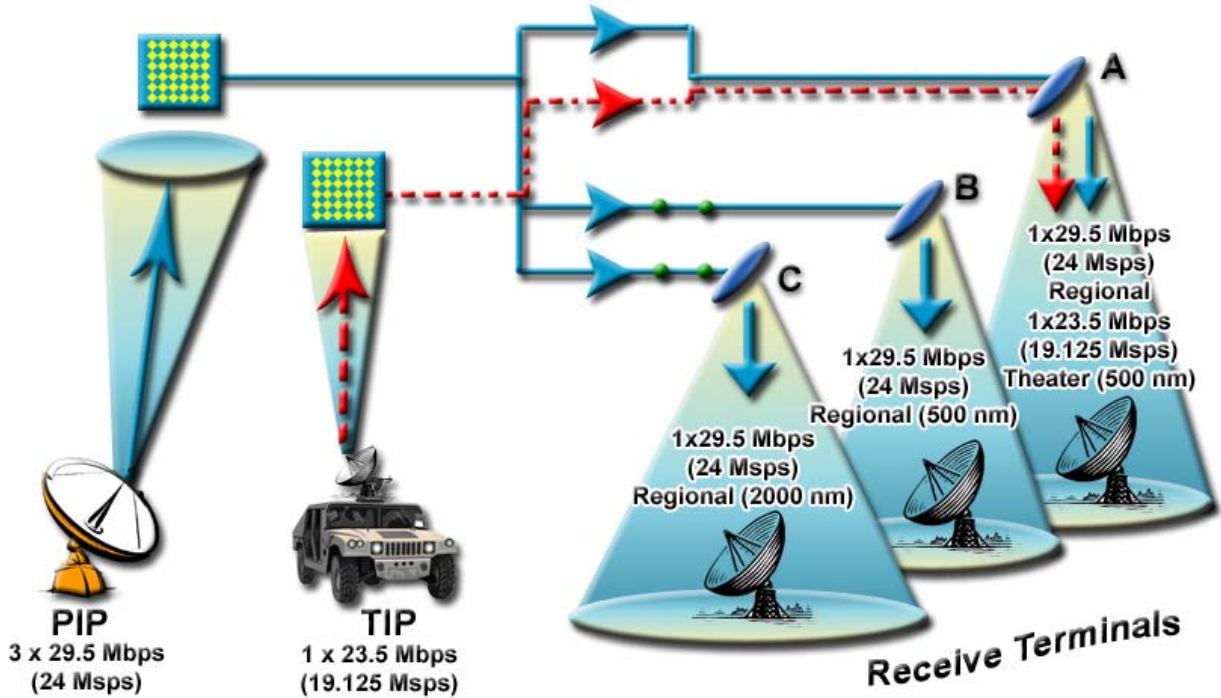
spot and one broad area coverage). Each transponder can be connected to either uplink antenna (one at a time). For downlinking, two transponders are connected to one spot beam antenna. The third transponder is connected to the second spot beam antenna. The fourth transponder can be switched between the second spot beam antenna and the broad area coverage beam antenna. Figure 5-16 illustrates this configuration.



**Figure 5-16**  
**UFO GBS Payload Configuration**

Under COCOM direction and SBM control, downlink antennas on UFO/G can be moved (pointed) to deliver the broadcast stream to dispersed users across the satellite's FOV. Antenna pointing may take up to 10 minutes to complete. Several arrangements of uplinks and downlinks are possible based on the needs of the Warfighter. The following paragraphs are a few illustrations of GBS support on UFO/G satellites:

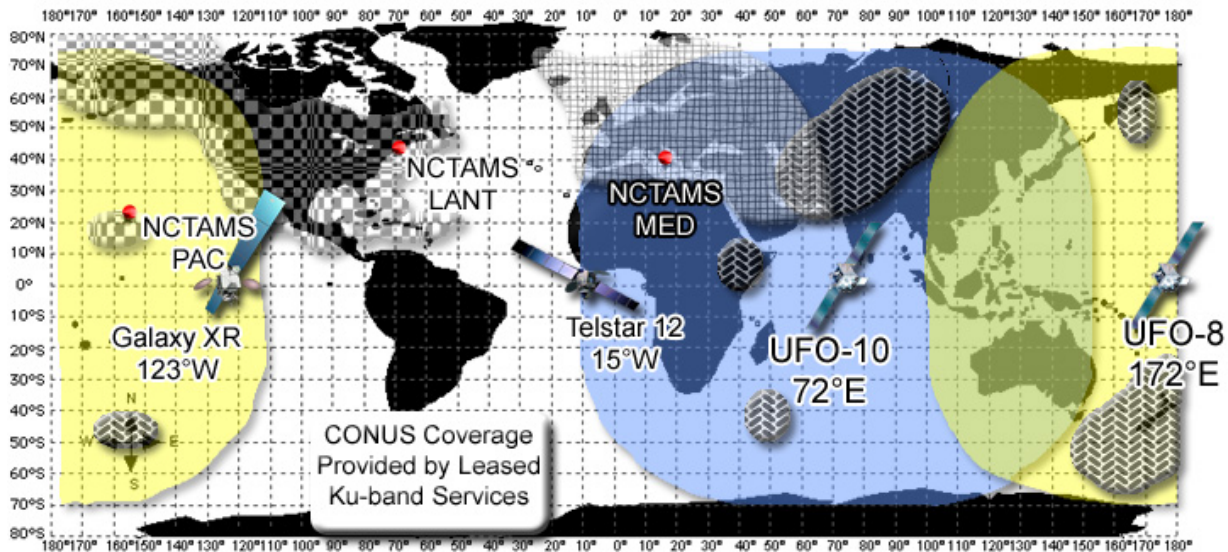
The PIP injects a broadcast into the fixed uplink antenna for three of the four transponders (three at 29.5 Mbps [24 Mbps]). On the satellite, two transponders operating at 29.5 Mbps (24 Mbps) (one to each spot antenna) broadcast through separate 500 nm spot beams. A third transponder, also operating at 29.5 Mbps (24 Mbps) and switched to the broad area coverage antenna, broadcasts through a 2000 nm broad area coverage beam. The TIP injects a 29.5 Mbps (24 Mbps) broadcast into the steerable uplink antenna. On the satellite, a fourth transponder connected to (and sharing) the first spot beam antenna broadcasts through a 29.5 Mbps (24 Mbps) spot beam. With this payload configuration, the 500 nm spot beam with transponders injected by both the PIP and TIP would point toward the same location and forces in that location could receive both broadcasts. See Figure 5-17



**Figure 5-17**  
**Example UFO/G Configuration A**

Figure 5-18 shows the nominal locations of UFO 8 and 10 with their FOVs at 10° elevation. It also provides sample spot beam coverage locations and shows the locations of the SBMs at the various Naval Computer and Telecommunications Area Master Station (NCTAMS) sites.

Coverage for CONUS and LANT will be provided by commercial augmentation satellites until WGS coverage is available. WGS satellites, when launched, will augment this coverage area.



## Coverage @ 10° Elevation

### Legend




- Sample UFO Spot Beams - 
- Telstar Coverage - 
- Galaxy XR Coverage - 

Figure 5-18

### GBS UFO/G Phase 2 Coverage with Sample Beam Locations

#### 5.2.11 TELEVISION DIRECT TO SAILOR (TV-DTS)

Television direct-to-sailors (TV-DTS) bring enhanced SA and quality-of-life programming to Sailors and Marines at sea. The TV-DTS program provides capability for a continuous worldwide Armed Forces Radio and Television Service (AFRTS) television, audio, and data broadcast to Navy forces. TV-DTS is a Navy-funded initiative and provides major networks such as CNN and ESPN broadcast via C-band with nearly worldwide coverage television and radio programming obtained by, and generated from, the AFRTS broadcast center. The installed system includes:

1. Video Channel One – ABC, CBS, CNN, Fox, NBC/News Programming
2. Video Channel Two – ABC, CBS, CNN, ESPN, Fox, NBC/Sports Programming
3. Video Channel Three – ABC, CBS, CNN, Fox, NBC/Entertainment Programming
4. Four radio channels – Music, News, Live Sports, Information

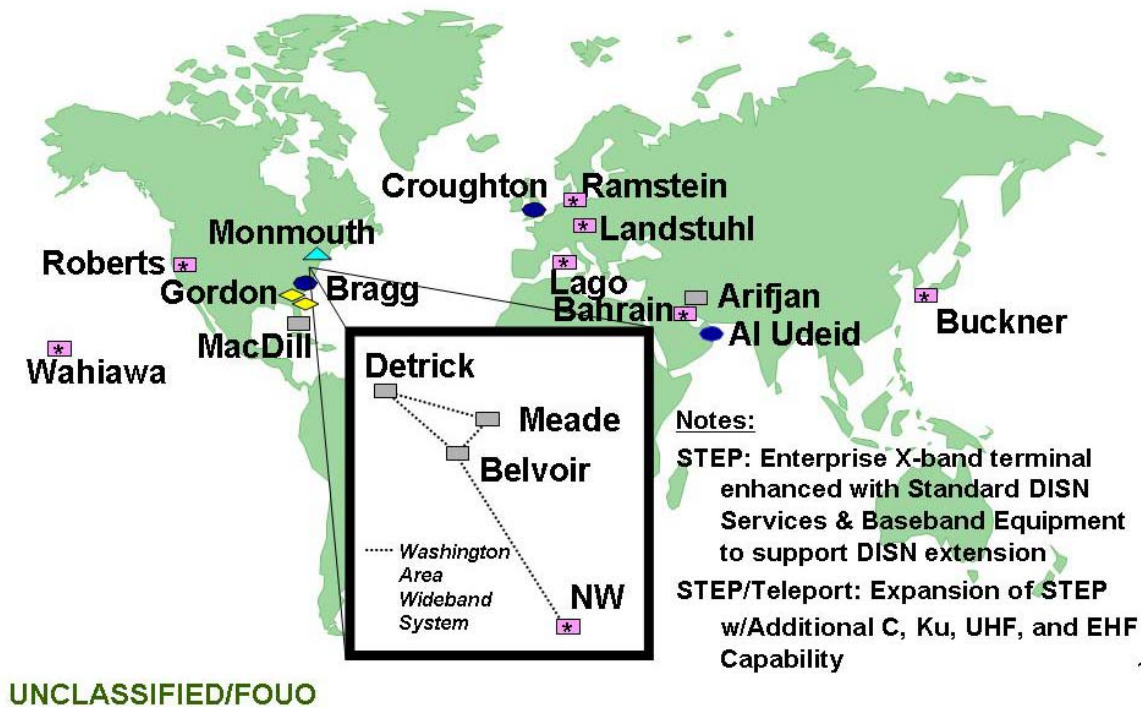
5. Data Channel – 24-hour news feed: Early Bird, NAVNEWS, Stars and Stripes, Times Fax.

TV-DTS uses C-band commercially leased frequencies to broadcast a 3.6 Mbps signal to shipboard terminals with a 1.2 meter receive-only antenna. Shipboard terminals also have a Ku capability to receive satellite television broadcasts directly from commercial providers such as Direct TV, Dish Network, etc. AFRTS programming originates from facilities at March AFB, CA, and is relayed to uplink facilities located in CONUS east and west coast, and Europe.

#### **5.2.12 DoD Gateways**

DoD Gateways are a collection of STEP and DoD Teleport facilities providing worldwide ground entry interface to space segment resources. The DoD Teleport program capitalizes on the current STEP sites to meet the warfighter's needs by providing a robust system with gateway access to SATCOM resources and Global Information Grid/Defense Information Systems Network (GIG/DISN) services. Joint and service-level operational users rely on both military and commercial SATCOM systems to support their operational Command, Control, Communications, Computers and Intelligence (C4I) requirements. Gateway sites established by the DoD Teleport program enhance access to military and commercial SATCOM resources, improve interoperability of Joint communications systems, and support seamless accessibility to the GIG by the JTF, Joint deployed headquarters, and deployed forces. The DoD Gateway utilizes the STEP System and DoD Teleport capability enhancements to provide additional SATCOM systems coverage and robust GIG/DISN services. Accesses to DISN services are via multi-media Radio Frequency (RF) connections. This multi-media RF includes existing SATCOM systems (i.e., Super High Frequency (SHF) (DSCS X-band), UHF, and EHF), future Ka, as well as commercial SHF Wideband systems in the C and Ku bands. The Gateway consists of the Service Delivery Node (SDN) providing connections to the Defense Switched Network (DSN), DISN Video Services (DVS), Defense Red Switched Network (DRSN), and the Joint Worldwide Intelligence Communications System (JWICS). Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) services are provided via the ITSDN.



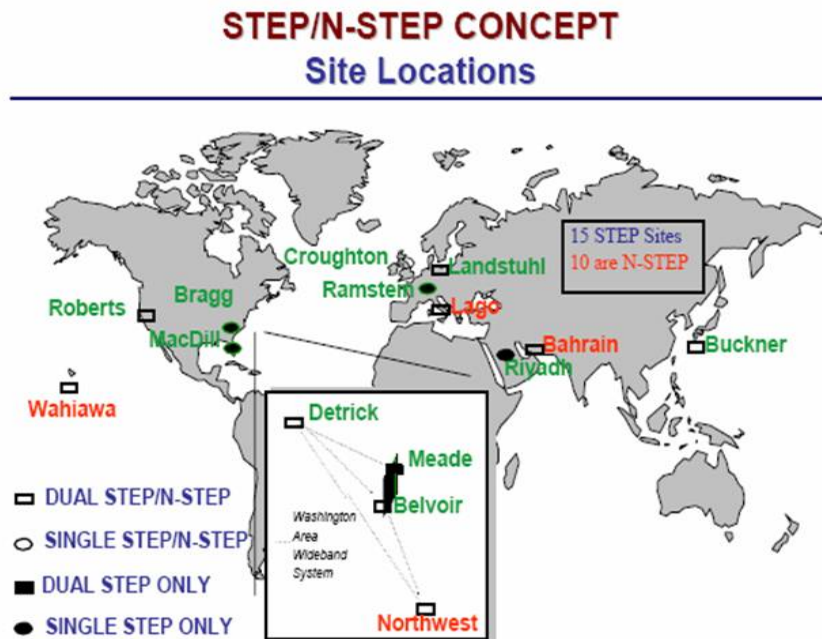


**Figure 5-19**  
**DoD Gateway Locations**

The STEP concept was developed to provide all tactical warfighters Joint operability and seamless integration to strategic NCA and in-theater C4I access and services. The establishment of the STEP program provides a standard set of pre-positioned C4I services at pivotal ground-entry stations (i.e., gateways) worldwide, as well as interoperability and standardization between the Services.

STEP sites, in addition to providing access to DISN C4I services, also provide Tri-Service Tactical Communications (TRI-TAC) switch interfaces for GMF and Joint Maritime terminal users and Joint Maritime User (JMU) access through the Automated Digital Multiplexing System (ADMS) to Navy C4I communications ashore. The equipment at the DSCS gateway includes the tactical baseband equipment necessary to interface the DSCS Earth terminal to the DISN. That portion of the STEP program initiative to provide JMU access through STEP sites to Joint Voice and Data Networks (JVDN) services, joint force interfaces, and/or Navy ADMS is commonly referred to as N-STEP. JVDN services include Defense Switched Network (DSN) and Defense Red Switch Network (DRSN) for voice; Nonsecure Internet Protocol Router Network (NIPRNET); Secret Internet Protocol Router Network (SIPRNET); JWICS for special intelligence (SI) data and video applications; and VTC for common-user video.

There are 15 STEP sites that provide worldwide coverage; of those 15, 10 sites are designated as N-STEP. There are at least three STEP sites, including one dual STEP site, located within each of the five DSCS satellite coverage areas. However, only four of the five DSCS satellite coverage areas are supported by three or more N-STEP sites (two in WPAC). Each N-STEP has, in addition to the normal STEP configuration of equipment, a complement of modems (ComQuest CQM-248A/SLM-3650), second level multiplexers (AN/FCC-100), TRANSEC (KG-194), and ADMS network multiplexer (TIMEPLEX Link/2+) equipment to support the N-STEP mission. Although a standard set of JVDN and interoperability services are provided, STEP/N-STEP sites may be configured differently. A single STEP site supports an Earth terminal that views one DSCS satellite; a dual STEP site supports two Earth terminals at one site, each viewing a different DSCS satellite. Figure 5-20 shows the STEP site locations.



**Figure 5-20**  
**STEP site locations**

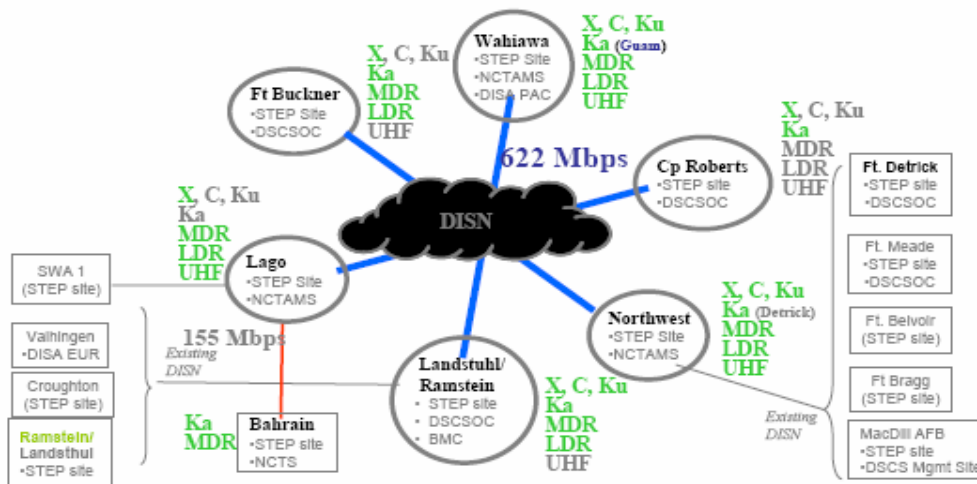
### 5.2.13 DoD TELEPORT

The Defense Information Systems Agency (DISA) is implementing the Department of Defense (DoD) Teleport System. The system will integrate, manage, and control a variety of communications interfaces between the Defense Information System Network (DISN)

terrestrial and tactical satellite communications (SATCOM) assets at a single point of presence.

The system is a telecommunications collection and distribution point, providing deployed warfighters with multi-band, multimedia, and worldwide reach-back capabilities to DISN that far exceed current capabilities. Teleport is an extension of the Standardized Tactical Entry Point (STEP) program, which currently provides reach-back for deployed warfighters via the Defense Satellite Communications System (DSCS) X-band satellites. This new system provides additional connectivity via multiple military and commercial SATCOM systems, and it provides a seamless interface into DISN. The system provides inter- and intra-theater communications through a variety of SATCOM choices and increased DISN access capabilities. Figure 5-21 depicts a notional DoD Teleport Architecture.

## DoD TELEPORT *Notional Architecture*



**Figure 5-21**  
**DoD TELEPORT Architecture**

### 5.2.14 JMINI (Joint (UHF) MILSATCOM Network Integrated Control System) / DAMA SAC II

Both the DAMA SAC and the JMINI IOC Control Systems (see Figure 5-22) enables communications between and among all UHF MILSATCOM users regardless of service or agency affiliation or user terminal equipment. Both systems provide centralized control and management of voice and data communications operating over 25Khz UHF channels. The JMINI IOC system also provides this same capability over 5-Khz channels. Both systems respond to requests from users, pre-assigned network requirements, and operator

commands to allocate access to available time slots on DAMA channels. Both systems allow for pre-planned and dynamically allocated UHF SATCOM assets to JCS-validated users of UHF SATCOM to support a variety of assigned tasks including theater communications, command and control, tactical communications, mobility and common user communications.

JMINI FOC (fielding began FY07) provides the following:

1. Centralized DAMA control of all available 25-Khz channels as either control or slave channels (and) 5-Khz channels as slave channels.
2. Provides DASA access capability.
3. Interface to new 4 channel DMR radios (up to 7 per footprint).
4. Centralized control of up to 28 home channels (25-Khz DAMA).
5. System redundancy for loss of radio, controller or channel.
6. Automated activation/deactivation of individual networks.
7. Demand assignment (ad hoc): 2 party, conference and network requests.
8. Interfaces to Network Management System (NMS) providing connectivity and remote monitoring between control sites, channel allocation and assignment managers via SIPRNET.

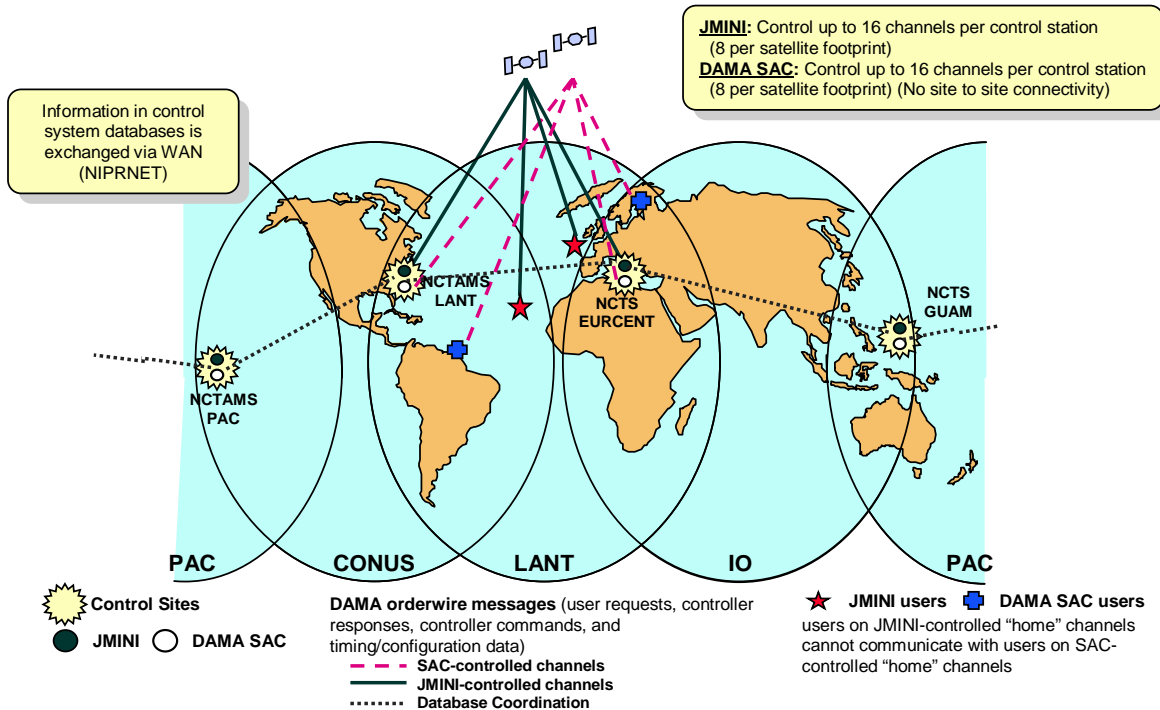
JMINI IOC will be retained to provide 5-Khz DAMA control.

DAMA SAC / TD-1271s / WSC 5 will be removed.

GCIB 25 provides a DAMA SAC and JMINI overview.



## DAMA SAC & JMINI IOC Control System Architecture



18

**Figure 5-22  
 DAMA SAC & JMINI IOC Control System Architecture**

### 5.3 SUBMARINE COMMUNICATIONS

#### 5.3.1 BROADCAST CONTROL AUTHORITY (BCA)

The Broadcast Control Authority (BCA) is the central hub where all message traffic sent to or received by submarines and shore stations gets disseminated. These facilities also provide troubleshooting expertise to units experiencing problems with any of a myriad of communications suites.

The BCA has established guidelines for discriminating between operational and non-operational traffic. Traffic that is non-operational (in that it doesn't affect the operational control or posture of the ship) is "screened off" the broadcast and placed into a file and deemed "ZFB-2" traffic. Operational traffic however is forwarded to the afloat unit by means of loading it into a message buffer or "queue". The unit can either actively request its traffic via a "Warrior Pull" or receive the traffic passively via scheduled passive downlink times.

Ships acquire their operational traffic by using the Information Screening and Delivery Subsystem (ISDS). This circuit is established using ADNS and setup is primarily via an EHF RF path (UHF and SHF can also be used). While ZFB-2 traffic is not placed on the Submarine's broadcast, it can be accessed using ISDS. It's recommended that units download their ZFB-2 traffic at sea whenever operational feasible, so as not to backlog messages which would then require downloading and routing upon return to home port.

The BCA monitors chat rooms to assist in troubleshooting, pass operational intents, or any other data at a near real-time pace. Chat enables resolution to operational problems (water space management, material issues, etc) as well as personnel problems (medical advice, AMCROSS discussions, etc).

The BCA monitors UHF Voice Circuits and monitors the Worldwide Submarine Net 668 (EHF voice). This voice net is accessible by any submarine. It is continuously monitored by BCAs in all AORs. This circuit is used for coordination between afloat units and BCAs, usually regarding submarine broadcast problems or discrepancies.

### **5.3.2 BASE CONSOLIDATED TELECOMMUNICATIONS CENTER (BCT)**

The Base Consolidated Telecommunications Center (BCT) is a local entity available at Subases whose role varies slightly depending on which theater it's located in, upgrades to equipment, etc. The BCT provides traffic via an in port routing system called "Gateguard" which requires direct interaction between the afloat unit and the BCT. The afloat unit receives message traffic from the BCT via a secure telephone line and then disseminates the traffic using Gateguard and ship's Local Area Network (LAN). The BCT is strictly a back-up means of processing incoming and outgoing traffic for the afloat unit in the event that the unit loses ADNS connectivity (hence ISDS) due to equipment or other material problems.

In the event that the unit has problems receiving their traffic via IADS and it appears that there will be a substantial loss of message traffic incurred, the unit should draft a COMMSHIFT message addressing the concern and send it to the cognizant BCA. The COMMSHIFT will request that the BCA redirect all message traffic for the unit to the local BCT via the ISDS server until ISDS resolution can be established.

### **5.3.3 SUBMARINE BROADCAST SYSTEM**

Messages delivered via the submarine broadcast are limited to operational and time-sensitive messages as determined by the BCA. Naval messages sent to submarines are received first by the BCA, The BCA assigns a sequential broadcast sequence number (BCSN) to uniquely identify each message placed on the broadcast. At the

start of each broadcast schedule, a list of all messages on the schedule (called a ZBO) is transmitted. The ZBO includes the BCSN, message precedence, transmission number, addressees, approximate transmission time using 50 baud, and a list of previously transmitted messages (ZRR). Each submarine is required to account for every BCSN on its assigned broadcast by copying all messages addressed to them or determining that a BCSN is of no interest because it is not addressed to them. If a message is missed, the submarine must contact the BCA to request a retransmission, or reprotect for the message.

Message traffic profiled to the Active folder will run on the Submarine IP ISDS broadcast based on the assigned broadcast and duration designated in the ship's SUBNOTE or Weekly OPSKED. The duration of a submarine broadcast schedule is 2 hours. The exact number of schedules depends on current operations and can vary from 4 schedules (8 hours) to as many as 12 schedules (24 hours). Generally a message will be broadcast for 6 schedules (12 hours). Messages profiled into the deferred folder are available via Warrior Pull only. Messages may also be transmitted via VLF broadcast or just the ZBO itself can be on the VLF broadcast. Submarines are required to line up with the VLF broadcast during each communications period. Figure 5-23 shows the Fixed Submarine Broadcast Architecture).

#### **5.3.4 VLF DIGITAL INFORMATION NETWORK (VERDIN) BROADCAST**

The VLF Digital Information Network (VERDIN) broadcast system provides a highly reliable and secure system for worldwide delivery of operational, tactical, and administrative messages from the Fleet Submarine Broadcast System (FSBS) and Minimum Essential Emergency Communications Network (MEECN). The Submarine LF-VLF VMEBUS / Receiver (SLVR) system is the receive side of VERDIN and includes the equipment necessary to receive VLF radio signals (between 14 kHz and 160 kHz), process the signals, and presents them to the operator in the form of an audio signal (continuous wave (CW)) or as a message on a teletypewriter page printer and tape perforator. The VLF/LF multi-channel submarine broadcast system is operable while the submarine is on the surface or at various operating depths with the multifunction mast, Type 18(v) or 15L periscope, BRR-6 Communications Buoy, or OE-315 Floating Wire Antenna employed.

The VERDIN broadcast system is capable of long distance (>600 nm) communications and is essentially an extension of the DCS, which connects the SUBOPAETH to submarines at sea. VERDIN provides worldwide coverage for the various submarine broadcasts from multiple transmitter sites. The system is normally operated in a four-channel mode, but it is capable of operating in a variety of modes that adapt system performance and characteristics to specified missions and operational doctrine.

### 5.3.5 VLF/LF SI VLF SECURE, NATO VALLOR, SI VALLOR CIRCUITS

The VLF/LF single-channel submarine broadcast (VALLOR) operates as a backup to the VERDIN system. The system provides for reception of Sensitive Information (SI) VLF Secure, North Atlantic Treaty Organization (NATO) VALLOR, and SI VALLOR narrative text messages over VLF/LF RF signals from the multifunction mast, Type 18(v) or 15L periscope, BRR-6 Communications Buoy, or OE-315 Floating Wire Antenna. The NATO VALLOR and SI VALLOR variation of these circuits require periods processing procedures during which the KWR-46 is reloaded with alternate cryptographic key material.

These circuits employ the SLVR to receive, demodulate, and de-multiplex the RF signal into separate digital baseband channels. Double encrypted SI VLF Secure messages have the first level of encryption removed by the SLVR. The second level of decryption occurs in the KWR-46 or is routed to the MLCS. NATO VALLOR and SI VALLOR channels bypass the SLVR.

### 5.3.6 INFORMATION SCREENING AND DELIVERY SYSTEM (ISDS)

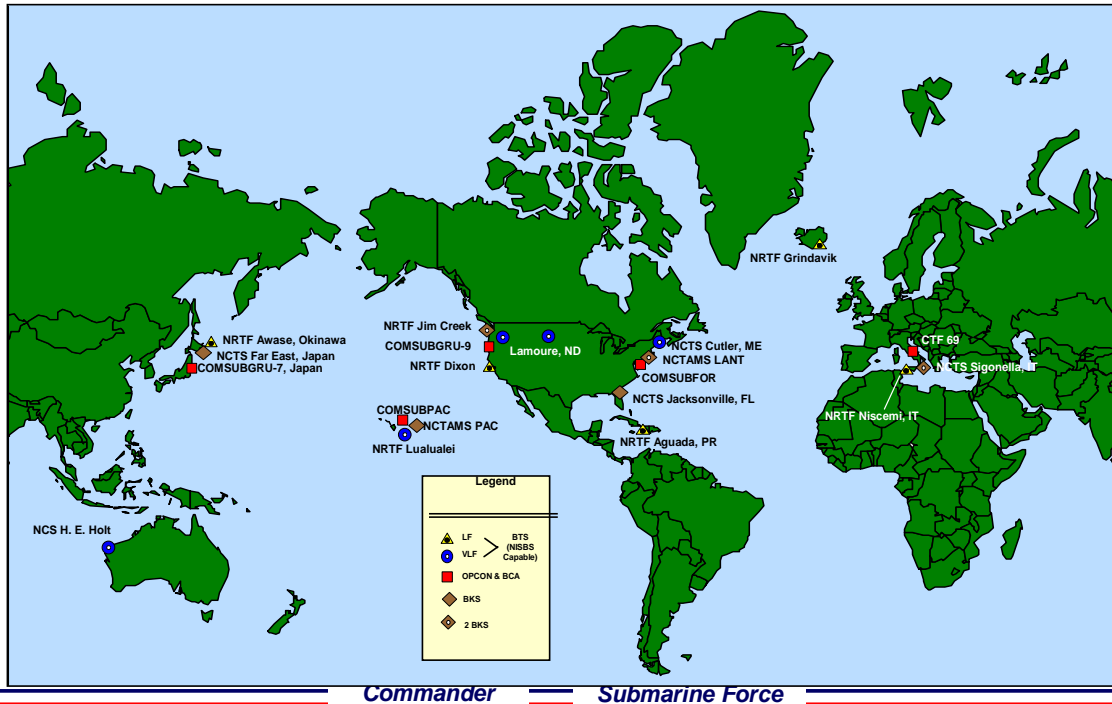
ISDS is the primary means for the transmission and reception of record message traffic between the submarine unit and the (Submarine Operating Authority) SUBOPATH's BCA via established IP communications paths. Additionally, ISDS is utilized for the verification of SATCOM IP Broadcast message accountability and the transfer of incoming message traffic to the Defense Messaging Distribution Subsystem (DMDS) for down hull distribution. ISDS utilizes a previously established IP circuit and is not dependent on one circuit or frequency spectrum. After the submarine has established an IP circuit and ISDS is configured to the active IP channel, ISDS will interface with the shore server for processing information. ISDS has two primary modes of operation:

1. Passive ISDS broadcast for the reception of message traffic.
2. Warrior Pull for the reception and transmission of message traffic and active query for the unit's message traffic pending at the Shore ISDS Server.





## Fixed Submarine Broadcast Architecture (LF/VLF)



**Figure 5-23**  
**LF/VLF Fixed Submarine Broadcast Architecture**

### 5.3.7 WARRIOR PULL

Since ISDS is an IP based system it has the ability to request information on demand as opposed to having it continuously broadcast. A Warrior Pull functions much like loading a web page on the World Wide Web in that the information is not sent until it is requested. When information is broadcast without a request it is referred to as a Smart Push. A GBS video broadcast for a specific mission would be an example of a Smart Push.

It is possible to Warrior Pull for ZBO traffic at any time EMCON conditions allow. If traffic is received via a Warrior Pull the ship should verify receipt of all applicable messages on the ZBO and acknowledge receipt so the BCA may remove them from ship's message queue and prevent sending them again. It is faster to receive message traffic on a passive ISDS broadcast than to Warrior Pull for it.

### 5.3.8 HF VALLOR CIRCUIT

HF Vallor is a receive only circuit which provides for the

reception of record and tactical messages over an HF data circuit by the submarine within or beyond LOS range from the transmitting platform. A data signal is converted to an audio signal at the transmitting station and converted back to a data signal at the receiving station. Data is provided at a rate of 50bps.

### 5.3.9 SUBMARINE SHIP / SHORE / SHIP CHECK REPORT

Submarines are required to make regular position check reports. Check reports are unclassified messages, assigned IMMEDIATE precedence, to ensure safety accountability of the reporting submarine. These reports are identified by the code word CHECK after the UNCLAS. Proper and expeditious handling is necessary since delays and non-deliveries may result in extensive search operations, e.g., SUBMISS, SUBSUNK.

#### SAMPLE SUB CHECK REPORT:

O 121901Z MAR 00  
 FM USS GREENMAN  
 TO COMSUBGRU TWO  
 INFO COMSUBRON TWO  
 COMSUBLANT NORFOLK VA  
 BT  
 UNCLAS  
 CHECK TWO FOUR SUBMARINE GREENMAN  
 BT

Submarine traffic, by virtue of its urgent nature and need for quick transmission, has precedence over that of surface units, except for surface ships having FLASH traffic. When both submarines and surface units have FLASH or IMMEDIATE traffic, the submarine has precedence over the surface unit for messages of the same precedence. Submarines will identify themselves by stating SUBMARINE in the initial call-up. If submarines are unable to establish communications with shore stations, they are authorized to enter a task force or group (TF/TG) operations or administrative net using ship/shore operating procedures. The TF/TG NECOS will afford the submarines the same preferred treatment as shore stations and will accept the traffic for relay.

### 5.3.10 IP COMMUNICATIONS

Understanding the relevance of IP Communications is extremely critical to successful submarine operations. Carrier and Expeditionary Strike Group Commanders along with Joint and Coalition Commanders utilize IP Communications extensively. When deployed with a CSG or ESG, it is imperative that submarines establish ADNS connectivity during each periscope depth (PD) trip to ensure all tactically relevant information is onboard. IP Communications enable the expeditious transfer of operational information, the ability to obtain screened-off (ZFB-2) message

traffic, web access to intelligence, weather, training, and Strike Group data in addition to other tactical and strategic related information and resources.

Submarines utilize the External Communications System (ECS) and the ADNS to establish IP connectivity with the servicing SUBOPATH over RF satellite communications circuits. There are several pathways for establishing IP connectivity. These include UHF DAMA Asymmetric, EHF Asymmetric, UHF MCAP, EHF MDR, and GBS. Figure 5-24 shows the current Submarine IP Architecture while Figure 5-25 shows the future Submarine IP Architecture.

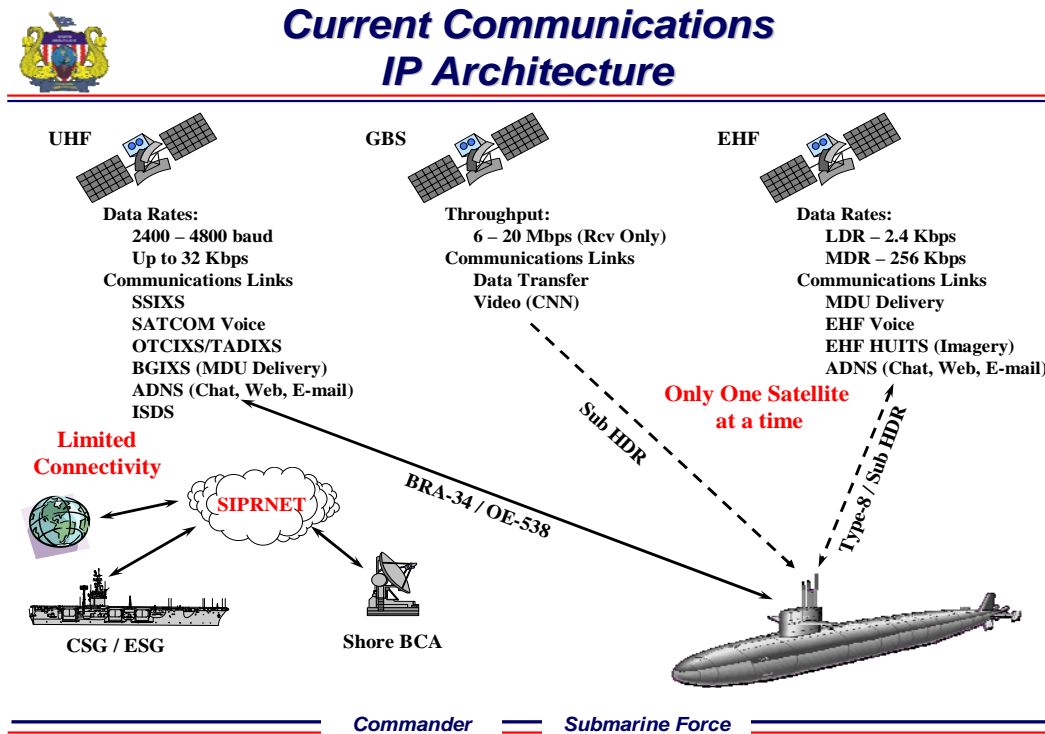


Figure 5-24  
Current Submarine IP architecture



## Future Communications—IP Enabled

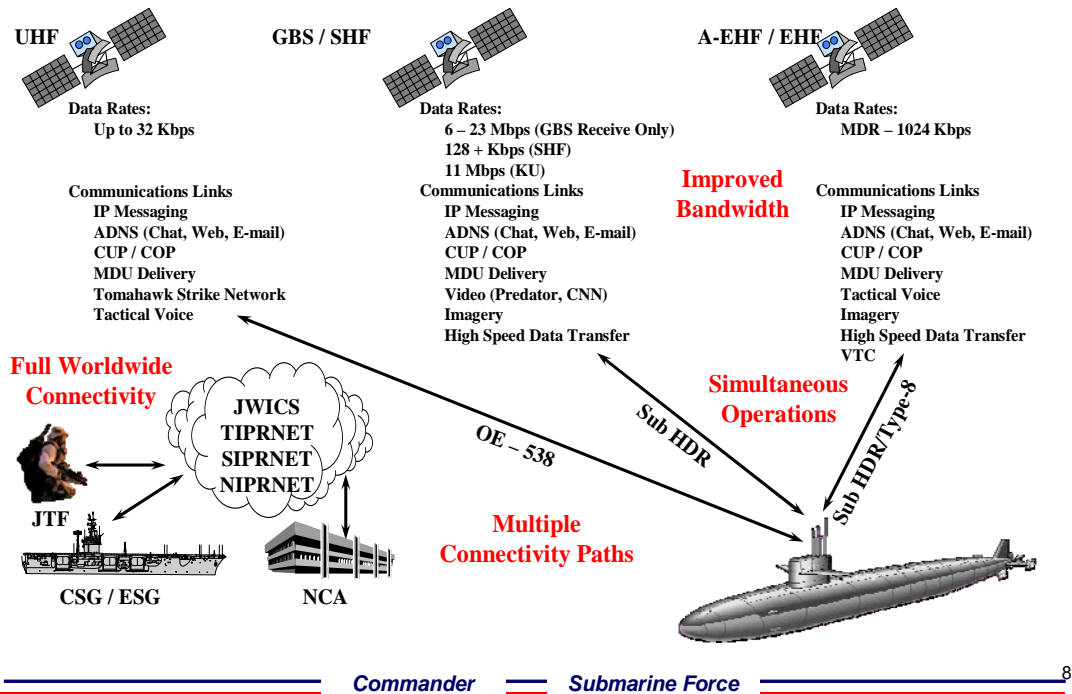


Figure 5-25  
Future Submarine IP architecture

## CHAPTER 6

### BASIC COMMUNICATIONS

#### 6.1 GENERAL

As with all human endeavors that require the interaction and cooperation of two or more people to achieve a common goal, effective communicating depends on procedures and terminologies which are familiar to and practiced by all. This section discusses the ship/shore and ship/ship procedures and terminologies that are standard to the NTS. CIB/CIA's document those specific communications procedures which vary from one ocean area to another.

Due in part to the increased bandwidth and availability afforded by UHF multiplexing systems such as the Demand Assigned Multiple Access (DAMA), assigned and on-call ship-to-shore circuits have migrated from HF to the UHF satellite frequency spectrum. However, HF ship-to-shore capability is still a viable, (albeit less reliable given HF susceptibility to natural and man-made interference), method of communications. CIB's and CIA's detail specific media and procedures available for ship-to-shore circuits in a given NAVCOMMAREA.

#### 6.2 SHIP / SHORE CIRCUIT MODES OF OPERATIONS

The three methods of operating circuits: simplex, duplex and semi-duplex, are described below. The particular mode of operation in use at any given time is dependent upon equipment and usable frequency available.

##### 1. SIMPLEX

Simplex is that type of operation which provides a single channel or frequency on which information can be exchanged. Simplex operation is normally reserved for UHF and those ships which do not have sufficient equipment for duplex operation. In some cases, a simplex circuit may be established when equipment casualties occur.

##### 2. DUPLEX

Duplex describes a circuit designed to transmit and receive simultaneously. In such operations each station transmits on a different frequency and both stations transmit concurrently.

- a) Full duplex (FDX) is defined as that type of operation which provides two channels or frequencies linking two stations, allowing the

simultaneous exchange of information;

- b) Half duplex (HDX) is that type of operation which provides unidirectional electrical communications between stations.

### 3. SEMIDUPLEX

Semi-duplex circuits are a combination of the simplex and duplex modes. All stations except the NECOS transmit and receive on the same frequency. The NECOS transmits, and is received on a second frequency. The NECOS may transmit continuously, whereas all other stations must transmit per simplex procedures.

## 6.3 FULL PERIOD TERMINATION

Full period terminations are dedicated circuits which provide communications between commanders afloat and those ashore. These terminations require allocation of limited NCTAMS/NAVCOMTELSTA assets. Therefore, the criteria for requesting, approving and establishing such circuits is necessarily strict, and must be reported by official message.

Afloat commanders and individual units may request full period terminations during special operations, deployments, intensive training periods or exercises when primary ship/shore will not suffice. But only when traffic volume exceeds speed and capability of ship/shore circuits, operational sensitivity requires circuit distinctness, or effective command and control necessitates dedicated circuits should commanders/units request a full period termination.

There are four types of full period terminations:

1. Single channel radio teletype (FSK/1K24F18) using either radio path or landline transmission media.
2. Single channel low data rate (LDR) satellite access (75 BPS DPSK) using satellite transmission media.
3. CUDIXS satellite access (2400 BPS DPSK) for NAVMACS equipped ships, using satellite transmission media.
4. Multi-channel radio teletype using TDM 1251 and SHF satellite transmission media.

### 6.3.1 FULL PERIOD TERMINATION REQUESTS

The heavy demands placed upon NCTAMS/NAVCOMTELSTA's for full

period terminations mandate maximum cooperation between shore stations and afloat commanders, both prior to and during an operation. Units having a need for a full period termination, either for training or operational requirements, will submit a termination request to the COMMAREA NCTAMS at least 48 hours prior to activation time. Emergency commitments or a command directive may necessitate a lead-time less than 48 hours. However, whenever possible, honor the two day limit to achieve maximum preparation and coordination. DO NOT address COMNAVNETWARCOM on these messages.

Termination requests will contain, but need not be limited to the following:

PRECEDENCE/DATE-TIME-GROUP  
 FM REQUESTING UNIT  
 TO COMMAREA NCTAMS  
 INFO ALT NCTAMS  
 NUMBERED FLEET COMMANDER  
 FLTCOM  
 BT  
 CLASSIFICATION //N02700//  
 MSGID/GENADMIN/REQUESTING UNIT//  
 SUBJ/TERMINATION REQUEST//  
 REF/A/DOC/COMNAVNETWARCOM/01JAN08//  
 AMPN/NTP 4(E) PARA 6.3  
 RMKS/1. IAW REF A, REQ FOL TERM:  
 A. TYPE TERMINATION (NOTES 1)  
 B. POSITION/LOCATION (NOTE 2)  
 C. MODE OF OPERATION AND KEY LIST (NOTE 3)  
 D. REQUESTED TERMINATION STATION (NOTE 4)  
 E. DURATION OF TERM (NOTE 5)  
 F. BROADCAST CHNL(S) COPIES (NOTE 6)  
 G. SPECAT CERTIFICATION (FULL TIME/  
 PRIOR NOTIFICATION) (NOTE 7)  
 H. REMARKS (NOTE 8)  
 DECLASSIFY AS APPROPRIATE//  
 BT

**NOTES:**

1. Describe termination required, listing multiple requirements in order:
  - a. Single channel or multi-channel UHF, landline, DSCS or tactical satellite (full duplex or simplex).
  - b. CUDIXS subscriber.
  - c. MINI-NET.
  - d. Secure or non-secure voice.

- e. Air/ground.
  - f. NCCS.
2. Estimated position or location at time of termination activation and projected area of operation during termination.
  3. Mode of operation and key lists:
    - a. FSK/DPSK, USKAT XXXX (If multi-channel, list channel assignment desired and individual key lists to be used).
    - b. 2400 BPS, DPSK, USKAT XXXX.
    - c. 75 BPS, DPSK, USKAT XXXX.
    - d. Others as appropriate.
  4. Terminating station will normally be assigned by the NCTAMS; however, a unit may specify the station with which termination is desired. If transiting COMMAREAS and a termination shift is requested, list stations, in order desired, specifying time of shift. For aircraft, indicate aircraft designation, ground NECOS and OPAREA.
  5. Indicate duration of termination with estimated start/stop dates/times.
  6. Indicate broadcast channels copied by individual channel designator.
  7. Indicate whether the commander concerned has certified that the receive terminal is cleared for SPECAT traffic full time.
  8. Remarks to include: embarked commanders, anticipated EMCON/RADHAZ/ECC drills, significant CASREPS affecting equipment limitations or capabilities and SPECAT certification.

The appropriate NCTAMS, upon receipt of the above message, will take the following actions:

1. Identify station(s) to which termination(s) are assigned, specify duration of termination and, if necessary, reason termination is not being assigned as requested.
2. Assign routing indicator.
3. Promulgate broadcast guard exemption, if applicable, or



assignment of broadcast channel for shore send side of termination.

4. Issue coordination instructions for activation of termination.
5. Provide information relative to proper submission of COMSPOT reports and Broadcast Service Requests.
6. Provide other information as necessary.

### **6.3.2 CIRCUIT ACTIVATION**

The shore station is the Net Control Station (NECOS) on full period terminations unless higher authority directs otherwise. As NECOS the shore station will ensure operators maintain strict circuit discipline at all times and perform duties outlined in paragraph 6.6. Once the NCTAMS has assigned the terminating shore station, the ship and shore station will begin coordination to identify specific equipment key lists and frequencies needed for the termination.

Prior to circuit activation, both units will ensure that all equipment is in peak operating condition. Equipment should be tested back-to-back or off-the-air to correct excessive distortion or other malfunctions. "Normal-through" equipment and channels should be used within the capabilities and/or limitations of the ship.

Two hours prior to scheduled termination coordinate with the ship using telephone, local circuitry, or Primary Ship/Shore to determine definite transmit/receive frequency assignments. If direct coordination with the ship is not possible, the shore station will send a message with all necessary information to the ship via the Fleet Broadcast. When the stations have established initial contact, they must verify channel assignments and crypto-cover for the circuits required.

If equipment tests are satisfactory one hour prior to circuit activation time, both ship and shore station will activate respective transmitters and receivers on the assigned frequencies. The shore station checks the frequencies to verify the transmitters are on the air, on frequency, and have a good quality signal. Upon activation of transmitters, both units will commence transmitting in cipher mode. When the ship or shore station is receiving a good quality signal, it will attempt to contact the other station for further coordination.

After the termination has been activated, the shore station

technical control facility will:

1. Maintain an up-to-date ship/shore status board;
2. Stay informed of the ship's position for proper antenna orientation;
3. Anticipate changes in propagation and ensure frequency changes are made to meet changing conditions;
4. Be responsive to ship's requests for timely shift of transmit frequencies.

### **6.3.3 MAINTAINING A FULL PERIOD TERMINATION**

The following actions apply to the ship and shore station when maintaining a full-period circuit:

1. Coordinate and jointly take action to prevent circuit outage regardless of cause. Action may involve shifting frequencies, allocating a directional antenna, or switching equipment.
2. Report and log all outages promptly, specifying reasons for outage and corrective action taken.
3. If the receive side of a duplex circuit is out, do not assume the send side is in the same condition. Continue to use the send side to pass information relative to circuit conditions. Continue transmission "in the blind" until it becomes apparent that the receiving station is not taking action on the corrective information, then attempt coordination by other means, i.e., the ship shall access ship/shore and the shore station shall transmit termination advisory messages via the broadcast. The number of messages transmitted under these conditions must not exceed 20 before the transmitting station obtains a receipt. In all cases, always send FLASH and IMMEDIATE, regardless of the number of other messages previously sent in the blind.

### **6.3.4 MESSAGE CONTINUITY**

Transmit messages first-in-first-out by precedence. Therefore, if a PRIORITY and IMMEDIATE are received together the IMMEDIATE will be transmitted first.

Number messages consecutively, starting at 0001Z each day regardless of crypto restart time. Automatic numbering

modules, if used at the NCTAMS/NAVCOMTELSTA and aboard ship, will be reset to 0001Z at the start of each new RADAY.

### 6.3.5 LOSS OF TERMINATION (SHORE)

When a termination is lost in either or both directions, shore station operators must take appropriate action and use every available means to re-establish the circuit, such as coordination via other shore stations maintaining terminations with ships in company, requests for transmitter and receiver support from other shore stations, etc. When circuit restoration procedures are unsuccessful, and/or a complete loss of communications exists, an IMMEDIATE precedence COMSPOT (see Appendix B) message will be transmitted. Ships will transmit these messages thirty minutes after initial outage and every two hours until restoration. The area NCTAMS will be an INFO addee along with other addrees as appropriate.

There are several ways to determine if the send side of a circuit is good or marginal, such as requesting a steady mark or dropping the transmitter off the air for short period (30 seconds) and bringing it back up. During periods of send outage, do not transmit longer than 10 minutes without testing and passing restoral instructions. Never shift both receive frequencies simultaneously. When one frequency is QRK 1/2 (the intelligibility of your signals is bad/poor.), it still may serve as a means of acknowledging instructions. These guidelines are not intended to suppress individual initiative in re-establishing lost communications. Circuit restoral is dependent upon timely action, quick decisions, and the ability of personnel to use any means available to restore communications in the shortest possible time.

### 6.3.6 TERMINATION SHIFTS

If a unit must shift terminations, securing the old termination/establishing the new termination should coincide with a broadcast shift whenever possible. Upon shifting or establishing terminations, submit a communications shift (COMMSHIFT) message per NTP 4 Supp 2.

NCTAMS will coordinate via existing circuitry with the involved shore station in its own COMMAREA or the receiving NCTAMS to affect the shift as follows:

1. The station with which the afloat unit is terminated will inform NCTAMS of transmit and receive frequencies in use at the time of desired shift to verify status board displays and avoid possible confusion.

2. NCTAMS will provide the NAVCOMTELSTA or adjacent NCTAMS with whom termination is desired of, current frequencies in use and obtain a report of signal strength and/or readability.
3. NCTAMS will direct the afloat unit to determine frequencies to be transmitted by the new terminating station. If frequency shifts are necessary, they will be screened and relayed by NCTAMS.
4. If equipment permits, the ship will maintain termination with the station from which the shift is being made until a quality traffic circuit has been established with the new termination. If this termination is not of traffic quality at the time of the shift, coordination may be accomplished via DAMA orderwire or Primary Ship/Shore.
5. When a traffic quality circuit has been established, the new terminating station will coordinate with previous terminating stations to secure the old termination.

Ships that have shifted their guard to a shore activity (COMMCEN) are not authorized access to satellite channels or HF terminations as these are retained for use by underway units. Transmit traffic by using GateGuard procedures. Strict compliance will be enforced by the appropriate NCTAMS using guard shift message and OPNAVINST 2300.42 as references.

### **6.3.7 TERMINATION CONTINUITY**

Continuity of a termination is the percent of time that at least one traffic channel of a trunk, excluding the orderwire, is available for use during a specified period of time. All general purpose traffic channels of a termination will be considered in computing continuity.

Commence continuity computations when the termination is activated both ways.

Example: A ship with three active traffic channels in a termination sustained outage on individual channels as follows:

Channel 2 - 1115Z-1330Z, 1745Z-1830Z and 2120Z-2250Z  
 Channel 3 - 1230Z-1400Z, 1840Z-1910Z and 2300Z-2330Z  
 Channel 4 - 1230Z-1330Z

Outage totals of 480 minutes were logged on all channels, but only 60 minutes of simultaneous outage on all channels

during 1230Z-1330Z would be considered as a trunk outage. Overall trunk continuity for the RADAY would be computed as follows:

Minutes that at least one channel in the trunk was usable for traffic

Continuity = Minutes that trunk was required to be active

$$\frac{(1440-60) \text{ min}}{1440 \text{ min}} = \frac{1380}{1440} = 96\%$$

Explain fully the daily outage periods attributed to equipment failure. Indicate whether the equipment failure occurred afloat or ashore. If the outage is attributed to equipment failure, indicate continuity of the next highest normal traffic channel not affected by equipment failure. Specify if personnel error contributed to total outage. It is important to remember that the receiving station controls the transmitting station's frequency shifts.

#### **6.4 PRIMARY SHIP / SHORE CIRCUITS**

Primary Ship/Shore (PRI S/S) circuits are encrypted, Frequency Shift Keying (FSK)/Phase Shift Keying (PSK) PC nets which permit afloat units to transmit record communications for delivery ashore. PRI S/S circuits can be accessed via the Navy Tactical UHF satellites. PRI S/S circuits are cleared to process classified traffic up to and including Top Secret. PRI S/S circuits may be used for coordination and establishment of full-period ship/shore terminations and are sometimes preempted for extension to fleet commanders during ASW command and control communications exercises or for other high priority usage.

##### **6.4.1 SHIP CALL-UP FOR PRIMARY SHIP / SHORE (DUPLEX MODE)**

The ship will ensure that the ship send frequency is not in use and that the shore send signal is tuned in and cryptographically in synchronization. When the send frequency is clear, turn on the transmitter and send a call-up, indicating the number and precedence of messages awaiting transmission and the shore send frequency which the ship is copying (e.g., 0810Z NAM DE NSWU ZBO IP/2R 6 K). The shore station may require the ship's position if a directional antenna is to be used.

After the called shore station has acknowledged the call-up and has indicated readiness to accept traffic, the ship will commence transmission of traffic as follows:

1859Z NPM DE NXXX 001/12 (Time ZULU, called and calling station, message being sent, RADAY,) (FL1 consisting of Start of Message function, the Last Three Characters of the ship's call sign and a four digit message sequential number) Continue with FL2 (RTTUZYUW RULYXXX0001 0120001-UUUU--RHMCSSU.)

A channel of the fleet multi-channel broadcast is used as an extension of the shore send side of PRI S/S circuits in certain NAVCOMMAREAS. This procedure provides ship operators with a continuous receive capability of the PRI S/S circuit. When making the initial call-up, the ship's operator must include the information that the ship is using the spare broadcast channels for reception, e.g., NAM DE NSWU ZBO 1P/2R ZRE CHNL 12 K. The shore station will respond on the spare broadcast channel. Consult NCTAMS CIB/CIA'S for additional details.

#### **6.4.2 SHORE STATION RESPONSE (DUPLEX MODE)**

The shore station will acknowledge ship call-ups and accept traffic or assign a turn number, e.g., 0811Z NSWU DE NAM QRY3 AR. The ship will then transmit traffic in the turn assigned by the NAVCOMTELSTA.

Prior to receipting for a message, the shore station must ensure a complete and correct message has been received. If possible, the NAVCOMTELSTA should correct format errors obviously resulting from "hits". If errors are in format line 2 (FL2), however, a rerun is generally required. After receipting for ship's traffic, the NAVCOMTELSTA will call-up for the next ship in turn.

#### **6.4.3 SHIP CALL-UP (HALF DUPLEX)**

The ship will ensure that the circuit is not in use, then will tune the transmitter and receiver to frequencies normally assigned for duplex operation. It will then perform a call-up as stated in duplex procedures except add "half-duplex" in the call-up.

#### **6.4.4 SHORE STATION RESPONSE (HALF DUPLEX)**

The shore station, upon receipt of a call-up indicating "half-duplex", will wait until the ship's transmitter goes off the air, will acknowledge the call, and will accept traffic as in duplex procedures.

#### **6.4.5 SHIP CALL-UP (SIMPLEX MODE)**

The ship will tune receiver and transmitter to the assigned frequency and ensure that the frequency is not in use. A call-up stating "simplex" is made. The transmitter must be turned off immediately following each transmission and, in no case, will transmitter tuning or transmission be accomplished when other units are actively using the frequency.

#### **6.4.6 SHORE STATION RESPONSE (SIMPLEX MODE)**

It must be recognized that when requesting simplex operation on duplex circuits, the shore station will acknowledge the call-up and accept traffic as in duplex procedures. On assigned simplex frequencies the shore station, after a fifteen-minute idle period, will transmit a one minute call-up.

#### **6.5 AUTOMATED MERCHANT VESSEL REPORTING (AMVER)**

AMVER is a computerized system for maintaining the dead reckoning navigation position of participating merchant vessels. Merchant vessels of all nations making coastal and oceanic voyages are encouraged to voluntarily send movement reports and periodic position reports to the AMVER center in New York via designated coastal, foreign, or ocean station ship radio stations. Any vessels between 80 degrees North and 80 degrees South worldwide may participate.

The AMVER center can deliver, in a matter of minutes, a surface picture (SURPIC) of vessels in the area of a SAR incident, including their predicted positions and their characteristics. This service is available to any RCC throughout the world where established communications links permit. In addition to all U.S. RCCs, SAR mission coordinators (SMCs) handling an oceanic mission of any type should always consider requesting a SURPIC regardless of whether it appears at the moment that merchant vessel assistance can be used. A SURPIC should be requested any time a mission is classified as in the distress phase or alert phase.

#### **6.6 NET CONTROL STATION (NECOS)**

The shore station is NECOS on all ship/shore circuits unless higher authority directs otherwise. NECOS for circuits which do not terminate at a shore station will normally be the

senior station/unit. This station/unit may in turn designate another station/unit on the circuit to function as NECOS. The shore station or other designated unit will assign fully qualified operators to perform the duties of NECOS. Positive and continuous circuit discipline is mandatory to prevent circuit inefficiency, confusion and transmission delay. Idle chatter, profanity, abusive language and spurious transmissions are absolutely forbidden. It is the responsibility of the NECOS to observe all violations and to take immediate action to eliminate the source. Repeated violators of circuit discipline will be reported to higher authority for corrective action.

The NECOS will establish the net with an initial transmission to ALL STATIONS THIS NET that contains the following instructions:

1. Identification of NECOS (ZKA).
2. Net operation (free or directed) (ZKB).
3. Order for answering - turn number (ZGB).
4. Any other special instructions (ZWC).

The net control station is charged with the following responsibilities:

1. Expedite traffic flow on the net.
2. Maintain circuit discipline.
3. Limit transmissions to the essential minimum.
4. Resolving disputes incident to message handling.
5. Determine procedural discrepancies and initiate corrective action.
6. Conduct a roll call of stations after each frequency shift, EMCON permitting.
7. Conduct a roll call of stations if the circuit is idle for 30 minutes or longer, EMCON permitting. On radio-telephone circuits, a station is understood to have good signal strength and readability unless otherwise notified. Strength of signals and readability will not be exchanged unless one station cannot clearly hear another station.
8. Limit control action to that which is required to immediately restore order. Amplification or exchange of information regarding a breach of circuit discipline must be sent via letter or message, rather than by



control circuits.

The NECOS will periodically monitor his own transmissions to ensure keying and cipher quality and frequency accuracy. As the shore station cannot possibly measure the accuracy of all ships' transmissions, it should only measure the transmission of ships noticeably out of tolerance, informing the ship directly of the discrepancy.

Authority of the NECOS extends to net operations within its scope of authority, and in this regard, all decisions of the NECOS are final. The NECOS does not have jurisdiction over the administration of individual stations within the net.

#### **6.7 FREE NET**

When operating conditions permit, the NECOS may direct that the net be operated as a free net. Member stations are thereby authorized to transmit traffic to other net stations without obtaining prior permission from the NECOS. Free net operation in no way relieves the NECOS of the authority and responsibility for effective circuit discipline.

#### **6.8 DIRECTED NET**

When operating requirements dictate that net stations obtain NECOS permission prior to transmitting, NECOS will control the net as a directed net. Directed nets are necessary when complicated traffic patterns or security factors exist and warrant direct control of each transmission. Transmission on a directed net may be accomplished per a predetermined schedule (i.e., turn numbers).

#### **6.9 ALTERNATE NET CONTROL STATION (ALTNECOS)**

The alternate net control station (ALTNECOS) will assume the duties of NECOS when directed or when NECOS has failed to answer after three successive calls. Upon assuming net control, the ALTNECOS will notify ALL STATIONS THIS NET (YAPD) that ALTNECOS has assumed the functions of the net control station by use of the operating signal ZKA (I am controlling station (net control station) on this frequency (or on ...kHz/MHZ)). Upon assumption of NECOS, the ALTNECOS will perform all duties carried out by the NECOS.

## 6.10 STATUS BOARDS

A central status board, (with classification markings as appropriate when filled in), will be maintained in the technical control area and should indicate as a minimum, all systems actually in use, systems tuned in or in standby status, and inoperative equipment. The accuracy of the information contained on the central status board will be verified by the supervisor(s) at watch turnover and at least once more per watch.

The following will be shown, as applicable, for active and standby systems:

1. Functional title of circuit.
2. Frequency(s), both send/receive if full duplex operation is employed.
3. Circuit designator, from communication plan.
4. Transmitter/receiver designations.
5. For shore stations, keying line designations.
6. Terminal equipment designations, e.g., AN/WSC-5 #1, etc.
7. Crypto equipment, keying material and restart time.
8. Operating position or remote control unit designations.
9. Remarks as appropriate.

For shore stations, the use of such words as active, inactive, on-call or standby to describe the transmitter/frequency status of Navy circuits has been replaced by the more definitive descriptions set forth below:

<u>CONDITION</u>	<u>TRANSMITTER STATUS</u>	<u>RESPONSE TIME</u>
ALFA - Continuously keyed broadcast and/or other frequencies with a receivable signal on the air	ON THE AIR CONTINUOUS	CONTINUOUS
BRAVO - transmitters/frequencies that are tuned and ready for keying. No signal on the air until transmitter is actually keyed	HIGH VOLTAGE ON	IMMEDIATE

CHARLIE - Transmitters/frequencies which can be activated within ten minutes.	HIGH VOLTAGE OFF	TEN MINUTES
DELTA - Transmitters/frequencies which can be activated within twenty-four hours.	COLD IRON	TWENTY-FOUR HOURS
ECHO - Transmitters down for repair. Use of this condition limited to NCTAMS reporting.	INOPERATIVE	INDEFINITE

**Table 6-1**  
**Transmitter/frequency status terminology**

In addition to the centralized status board, each circuit operator will maintain a status sheet at each individual operating position. This sheet will contain the following:

1. Circuit designation as listed in the effective communications plan.
2. Frequencies in use. (Not required at each position of a multi-channel system).
3. Address designators (call signs or routing indicators) and identification of all stations on the net.
4. Identification of NECOS and ALTNECOS as appropriate.
5. Status of all stations on the circuit, e.g., "IN", "OUT", EMCON, etc.

Each circuit operator will notify the supervisor when the circuit status changes, when a backlog of traffic develops, when an outgoing transmission is delayed, or when any deviation from prescribed procedures is recognized. When relieved, the circuit operator will pass-on information pertaining to the circuit(s), which is not covered in the circuit status information SOP'S.

#### **6.11 LOGGING OUT A CIRCUIT**

Due to propagation factors, there will be times when circuit conditions are such that the passing of traffic is either hindered or impossible. Technical Control should be notified as soon as a circuit begins to deteriorate. When a circuit has proved to be unusable for further message processing, notify the distant end to stop sending traffic (operating signal QRT) and to send test tapes. Also, notify

technical control to log the circuit out.

The decision to log out a circuit is, in many cases, an interpretive one and must be made carefully. For example, continual receipt of completely garbled messages or messages with numerous transmission hits warrants logging out of the circuit. However, one hit every few lines will not be sufficient cause to log out the circuit. Generally, the final authority for logging out a circuit rests with the fleet center supervisor, not the circuit operator.

Immediately after notification of log out, technical control assumes full responsibility for the circuit and all attending outage until circuit is restored to traffic quality. Technical control will ensure the distant station is testing on the circuit and will direct equipment adjustments and/or frequency shifts as required. Technical control will direct whatever measures are necessary to reestablish the circuit to traffic conditions. Under no circumstances will there be any circuit operator chatter, requests, or restoration attempts other than those directed by technical control.

When technical control restores the circuit to traffic quality, the circuit will be returned to the traffic section. The traffic section will then notify the distant end to send traffic. At this point of restoration and acceptance, it will be the responsibility of technical control to summarize to the user and to the distant end the time the circuit was logged down and up, the reason for outage (RFO) and any other pertinent information.

If a circuit is not restored within thirty minutes, a COMSPOT report, as outlined in Annex B, will be submitted.

#### **6.12 EMISSION CONTROL (EMCON)**

EMCON is control of all electromagnetic and acoustic radiations, including communications, radar, EW and sonar. During its imposition, no electronic emitting device within designated bands, including personal communications devices, will be operated unless absolutely essential to the mission. The OTC or his designated subordinate commander is responsible for imposing EMCON.

Operational requirements may require operating units to affect either full radio silence or HF EMCON. If at all possible, ships should notify the shore station of scheduled periods of EMCON due to radiation restrictions (HERO, HERF, RADHAZ) or others (man aloft, aircraft operations, etc.) prior to the actual restrictive period.

If EMCON is imposed without notice, relay procedures to deliver outgoing traffic may be attempted. Shore stations must be alert to the sudden, unscheduled imposition of EMCON and the accompanying lack of any transmissions from the ship.

If the ship should enter EMCON without prior notice, the shore station will keep a listening monitor on the ship's frequencies until the ship returns to the air. Additionally, a listening watch will be kept on the SATHICOM net for possible contact from the ship.

Once a ship with a multi-channel termination has returned to the air on previously assigned frequencies, the orderwire will be restored before the traffic circuits. If the ship maintains a single channel termination, the circuit will be reestablished via the technical control center.

If the EMCON period is of sufficient duration, the ship will notify technical control that it desires to secure the termination.

### **6.13 OPERATIONAL SHIPBOARD CIRCUITS**

In a Task Force/Task Group environment, a variety of intra-Task Force/Task Group circuits will be activated according to the dictates of the tactical situation.

Particular circuits to be activated will be as directed by the Officer in Tactical Command (OTC) in the communications plan. Ships expecting to deploy under the OPCON of a particular task organization commander will ensure that thorough preparations are made to comply with anticipated circuit requirements. Operation Orders and the Communications Plan should be reviewed as far in advance of actual deployment as possible.

The five most common Task Force/Task Group circuits are as follows:

1. Under Sea Warfare (USW) circuits, which can be either FSK or voice, are used to coordinate intra-Task Force/Task Group ASW actions.
2. Task Force/Task Group ADMIN circuits are used for administrative coordination.
3. Task Force/Task Group Broadcast circuits are used for rapid dissemination of information and are usually keyed by the flagship.
4. Task Force/Task Group common circuits are used to pass messages between units of the Force/Group or to pass traffic to a CUDIXS Special subscriber within the

Force/Group for relay to a NCTAMS.

5. The Fleet Warning/Tactical Net (277.8 MHz) is guarded continuously by all Navy ships (except submarines) when underway singly and by at least one ship of a group. Coast Guard cutters may use this frequency to communicate with Navy ships when required. The frequency may be particularly useful for navigational purposes during periods of reduced visibility when entering or leaving port if Navy ships are in the vicinity. The frequency is also used by the Navy for local ship/shore harbor communications on a secondary basis to inter-ship use. The OTC will designate one ship, normally the flagship, to guard this net.

The Fleet Warning/Tactical Net may be utilized:

- a. To establish communications between surface units and between surface units and aircraft:
- b. For promulgation (by the SOPA) of urgent warnings of natural disaster, such as hurricanes and typhoons.
- c. To pass emergency traffic.
- d. To pass operational traffic when no common communications plan is in effect.
- e. The Fleet Warning/Tactical Net will be guarded by all submarines while surfaced and in visual range of other fleet units (availability of equipment permitting).
- f. Normally, as a minimum, the circuit will be guarded on the bridge either as a loudspeaker watch or with full transmit capability as directed. Remote position watches in CIC or Main Communications will be activated as ordered;
- g. The Fleet Warning/Tactical Net will not be used for administrative matters. Circuit discipline on the net, as well as on all other radiotelephone circuits, is essential to the effective use of the net. Correct voice radio procedure is contained in ACP 125, with which all radiotelephone operators must be familiar.

#### **6.14 UHF AUTOCAT / SATCAT MIDDLEMAN RELAY PROCEDURES**

Shipboard HERO conditions and EMCON restrictions at times prohibit the transmission of radio frequency energy below 30 MHz. HERO refers to the hazard that electronic emissions may represent to ordnance during loading and off-loading operations. To provide an uninterrupted flow of essential communications without violating HERO and EMCON limitations,

techniques called AUTOCAT, SATCAT, and MIDDLEMAN were developed. With these techniques the range of tactical UHF circuits (voice or data) may be extended by relay of amplitude modulated UHF transmissions via HF or satellite. In AUTOCAT a ship and in SATCAT, an airborne platform provides the media for automatically relaying UHF transmissions. In MIDDLEMAN, the same objectives are obtained; however, this method requires an operator to copy the messages with subsequent manual retransmission.

Typically, a ship under EMCON or HERO conditions will transmit to a relay ship or aircraft on UHF. The relaying platform then retransmits the signal on another frequency to a terminated NCTAMS/NAVCOMTELSTA. Receiving techniques on the originating ship remain unchanged.

AUTOCAT, SATCAT and MIDDLEMAN use three different types of circuit configurations for reception and relay of UHF transmissions. These circuits are:

1. A voice circuit where some units send and receive on one frequency, and other units send and receive on any other frequency.
2. A voice circuit where all units transmit on one frequency and receive on another frequency.
3. A data circuit where all units transmit on one frequency and receive on another frequency.

#### **6.15 NON-ELECTRONIC RELAY SYSTEMS**

There are two other message relay systems, PIGEON POST and BEAN BAG.

Pigeon Post provides a method of traffic delivery to shore by aircraft while Bean Bag provides a method for small ships to deliver message traffic via helicopter to shore or to a unit that is terminated full period for further transmission.

#### **6.16 HIGH FREQUENCY - AUTOMATIC LINK ESTABLISHMENT (HF-ALE)**

The military standard HF-ALE radio is widely deployed throughout the US military and provides a viable alternative to over burdened satellite communication systems. Automatic Link Establishment (ALE) is an improvement to high frequency (HF) radio that allows establishment of considerable clearer over-the horizon voice communications and robust data transmissions.

ALE is a communication system that permits HF radio stations to call and link on the best HF channel automatically

without operator assistance. Typically, ALE systems make use of recently measured radio channel characteristics stored in a memory matrix to select the best frequency. The system works much like a telephone in that each radio in a network is assigned an address (similar to a call sign). When not in use, each radio receiver constantly scans through its assigned frequencies, listening for calls addressed to it.

Detailed information and procedures for HF-ALE operations can be found in NTP 6-02.6.

### **6.17 VERY HIGH FREQUENCY AND ULTRAHIGH FREQUENCY LINE OF SIGHT (LOS) COMMUNICATIONS**

VHF and UHF LOS communications support ship-to-ship, ship-to-shore, and ship-to-air LOS communications. Shipboard tactical VHF radios use the 30 to 88 MHz and 108 to 156 MHz segments of the VHF radio band for ship-to-shore communications in amphibious operations and for land-mobile shore communications. A portion of the VHF band (225 to 300 MHz) and the lower end of the UHF band (300 to 400 MHz) provide tactical ship-to-ship, ship-to-shore, and ship-to-aircraft radio nets. Havequick II and Link 4A also share the UHF spectrum.

VHF and UHF LOS communication systems use a variety of equipment. Only some of the equipment is transmitters and receivers. The majority fit into a category called transceivers – a combination transmitter and receiver that is generally compact, portable, and uses a single antenna. The following is a compilation of commonly used VHF and UHF LOS equipment and systems and their uses.

1. AN/ARC-182 VHF/UHF radio – A multiband/multimode radio (30 to 400 MHz) used for close air support, air traffic control, maritime radiotelephone, and NATO communications.
2. AN/GRT-21(V)3 VHF/UHF transmitter and AN/GRR-23(V)6 VHF/UHF receiver – Used for transmitting and monitoring aircraft distress communications (116.0 to 151.975 MHz) in the VHF range and for air traffic control (225.0 to 399.97 MHz) in the high VHF and low UHF range.
3. AN/URC-93 VHF/UHF LOS radio - Several configurations exist (225 to 400 MHz) that can be used with voice, electronic counter-countermeasures (ECCM), LPI, data, and wideband communications.
4. AN/VRC-40 series VHF radio – Used aboard ship as well as in vehicles (30 to 76 MHz) to support short range two-way VHF communications.



5. AN/WSC-3(V) 6 UHF LOS radio – The standard Navy shipboard LOS UHF transceiver (225 to 400 MHz) used for voice, data, and teletype (TTY).
6. AN/WSC-3(V)11 Havequick Transceiver – A modification of several existing tactical UHF radios for use in providing ECCM capability in the 225 to 400 MHz frequency range.
7. AN/URC-107(V)7 (JTIDS) – A high-capacity TDMA system that provides integrated communications, navigation, and IFF capabilities. It provides ECCM capabilities for aircraft and surface ships, extended range of communications, and OTH communications for surface ships with an airborne relay platform. It is also designed to accommodate secure voice and the digital information associated with Links 4A, 11, and 14.
8. Single-channel ground and airborne radio system (SINGARS) – A frequency-hopping, frequency modulating, spread-spectrum system (30 to 88 MHz) designed to provide SECVOX and data communications in jamming environments.

#### **6.18 DIGITAL WIDEBAND TRANSMISSION SYSTEM (DWTS)**

DWTS is a high-bandwidth, full-duplex, LOS UHF communications system designed primarily to support the USMC in intra-ESG distributed collaborative planning and ship-to-tactical shore network communications. It provides up to 2,048 kbps of multiplexed data throughput within the amphibious ready groups and provides interoperation with the USMC's AN/MRC-142 radios to support TRITAC voice and IP data. Via its interconnection to ADNS, it provides an alternate path for ship's IP data to effectively extend broadband satellite coverage to other ships within the ESG. Baseband systems supported by DWTS are the TSS for TRITAC compatible voice and ADNS for all network IP traffic and tactical VTC. The system consists of two radio suites on each ship that normally connect to each of the other two ships within the ESG, establishing a ring configuration. Automatic relaying by the baseband systems provides redundant paths within the ring. When interconnected to an MRC-142 ashore, the ring topology is broken and the closest ship connects to the Marine radio, which then provides a non-redundant connection between all ships of the ESG and the shore.

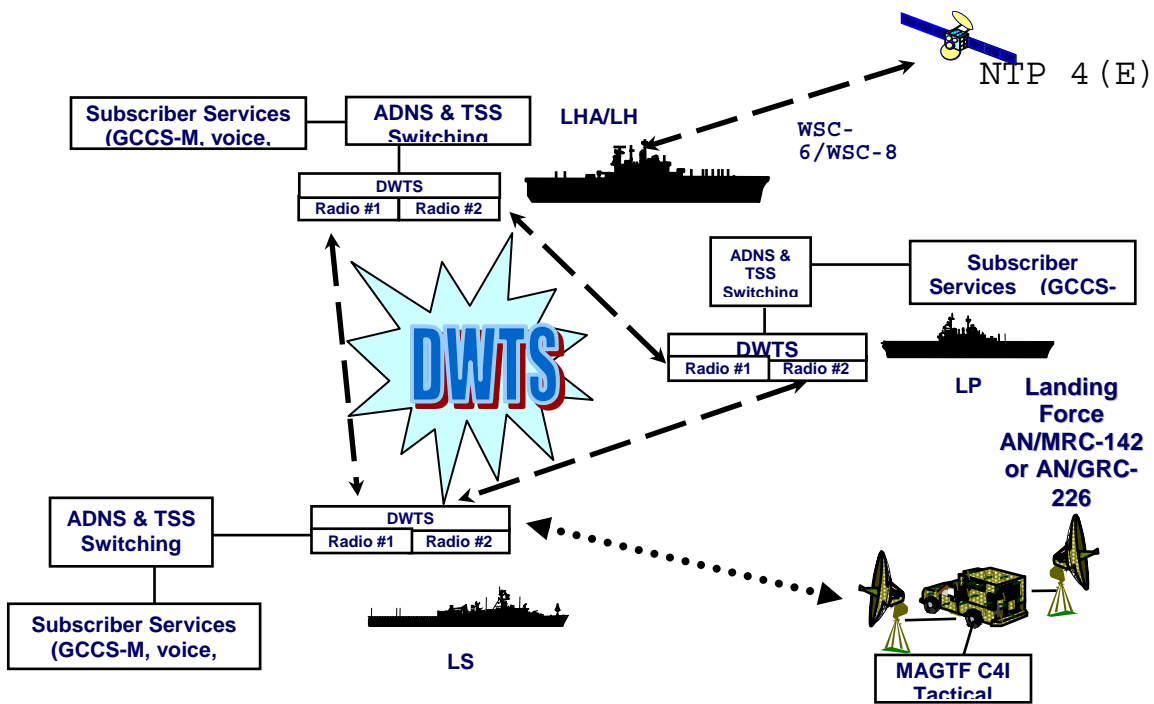


Figure 6-1  
DWTS

#### 6.19 TACTICAL SWITCHING SYSTEM (TSS)

The TSS (AN/SSQ-122(V)1) program provides ancillary baseband enabler equipment for SHF SATCOM terminals and UHF LOS wideband systems. It supports the exchange of tactical automated voice services between afloat joint commanders, landing force command elements at Marine regiment or Marine expeditionary unit (MEU) and higher, Army brigade and higher, and disembarked forces ashore. The TSS switched multiplex unit (SMU-96) and ancillary equipment (including automatic key distribution center (AKDC/HGX-93) provides the baseband switching for shipboard trunk interoperability with TRITAC equipment operated ashore, e.g., TRITAC switches, mobile subscriber equipment (MSE), GMF equipment, and transparent interface to commercial international networks. The TSS SMU interfaces include:

1. UHF LOS DWTS AN/SRC-57(V) for communications with USMC elements ashore and with non-SHF SATCOM capable amphibious ships.
2. SHF SATCOM AN/WSC-6(V)5 (2<sup>nd</sup> channel) for GMF communications via teleport/step gateways (LCC/LHA/LHD class ships).

The TSS is capable of handling a variety of TRITAC digital transmission groups (DTGs) (up to 4 standard DTGs with data rates up to 1152 kbps).

## **6.20 ENHANCED POSITION LOCATION REPORTING SYSTEM - DATA RADIO (EPLRS-DR)**

EPLRS-DR is a secure, spread-spectrum, frequency-hopping, UHF networking radio system. It provides digital communications for the Amphibious Force command element at the regiment to company level with reach back to the ESG. Via its connection to the ADNS, EPLRS-DR provides a 57.6 Kbps digital IP data path between command elements aboard ship and Marine networks ashore. Additionally, EPLRS provides the position location information of each radio, which is used to track and identify unit movement within the operational area for SA. The EPLRS-DR network is self-healing and provides automatic relaying up to six times for increased mobility and range extension. The radio utilizes synchronous TDMA, frequency division multiple access (FDMA), and code division multiple access technology, combined with embedded COMSEC for a secure, low probability of intercept, low probability of jamming RF-network. EPLRS provides interoperability with the Marine Corps, Army, and Air Force. Shipboard configurations will consist of one, three, and four radio suites depending on platform size and mission. A radio suite consists of the RT-1720 radio, antenna, MUTE interface (for LHD class ships), user readout unit, printer, EPLRS network manager (ENM) computer, power adapter, KOK-13 COMSEC equipment, and various mounts and interface adapters.

## **6.21 HIGH FREQUENCY (HF)**

Although the use of HF communications has diminished somewhat, it is making a resurgence in Naval communications. Allied and coalition communications, as well as some Emergency Action Message exercises, depend on HF services. Some special talent is required to optimize HF communications, but it is not that difficult as long as some basic concepts are understood. Frequency selection affects the success of HF communications to a greater degree than communications in other parts of the frequency spectrum. When a variety of frequencies are available for use, the frequency selected should optimize the chance of success in establishing the network. Frequency selection is influenced by such factors as time of day, propagation anomalies, local interference, and range. Higher frequencies are optimal during the day and lower frequencies are optimal at night. For example, if using HF in the middle of the day a frequency midway through the spectrum is optimum. These factors are considered when an OPTASK COMMS frequency plan is generated.

In the HF band, unlike all other tactical bands, frequency selection is everything. The optimal frequency is dependent on the ionosphere and time of day, as well as whether a Ground Wave or Skywave.

Ground Wave:

A ground wave is a radio wave on or near the earth's surface. The distance achieved by the ground wave portion of an HF signal depends on the type of terrain and the amount of transmitter power. Fortunately, the ocean's surface provides an excellent propagation environment which can permit reliable communications out to hundreds of miles with output power of as little as 100W in the lower end of the spectrum. However, higher frequencies will typically be quieter in regards to atmospheric noise. The rule of thumb is to select the highest frequency that will achieve the desired distance.

Skywave:

A skywave is a radio wave that is refracted back to Earth by the ionosphere, permitting transmission around the curve of the earth's surface.

The exact distances achieved by skywaves depend on the heights of the layers of the Ionosphere above the Earth. The heights of these layers are controlled by the season, the time of day, and the level of sunspot activity. Time and season are fairly easy to find. However, the sunspot cycle takes a little more research. Solar events tend to run in cycles of high and low activity, with peaks about every 11 years. The last peak was around 2001, with 2006 being in a trough. The basic rule is the higher the solar activity, the higher the sunspot number, the higher the ionization of the layers, and the higher the frequency for a given distance.

Ionosphere Layers:

*D Layer*- Lowest layer. This layer absorbs radio waves. Frequencies between 2 and 6MHz are very unreliable for daytime skywave communications.

*E Layer*- The next higher layer, it dissipates rapidly without direct sunshine. However, it can refract signals back to earth, albeit sporadically.

*F Layers*- F1 and F2, the highest layers are the most important to long distance communications. They remain ionized 24 hours a day, but more intensely in the daytime. At night the D and E layers disappear and the F1 and F2 layers combine into one layer. Higher frequencies will pass through these layers at night, but lower frequencies will be refracted back to Earth.

**6.22 VERY LOW FREQUENCY (VLF)**

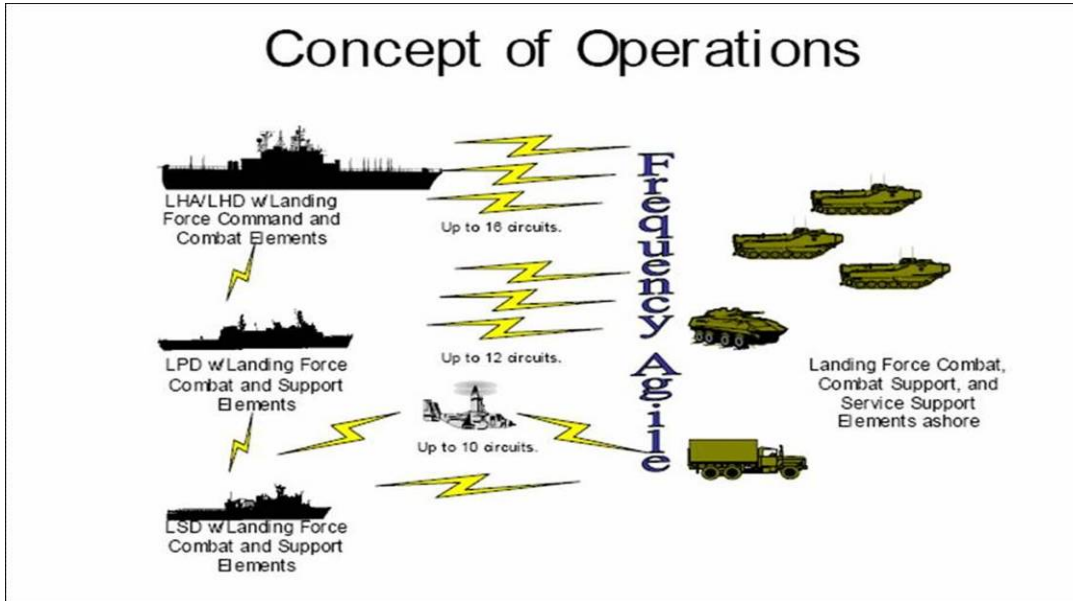
The Navy shore VLF/LF transmitter facilities transmit a 50 baud submarine C2 broadcast, which is the backbone of the submarine broadcast system. The VLF/LF radio broadcast provides robustness (i.e., improved performance in

atmospheric noise), availability, and global coverage and has seawater penetrating properties. The submarine VLF/LF broadcasts operate in a frequency range from 14 to 60 kHz and consist of six high-powered, multi-channel fixed VLF (FVLF) sites and seven multi-channel LF sites located worldwide.

The submarine VLF/LF broadcasts are generated by the BCA or alternate BCA from messages created locally by the C2 processor or the submarine/satellite information exchange system (SSIXS) processor, or accepted for relay by the submarine operating authority (SUBOPAETH). The BCAs and alternate BCAs are connected to the transmitter sites by dedicated inter-site links (ISLs) with the ability for the JCS and USSTRATCOM to seize BCAs, at any time, for EAM dissemination. At each of the transmitter sites, messages received over the ISLs are decrypted and input into the integrated submarine automated broadcast processor system (ISABPS). Submarine VLF/LF broadcasts a continuous transmission sequence of prioritized messages that normally lasts two hours. It is generated by ISABPS and sent to the VERDIN transmit terminal. The VERDIN transmit terminal is used to multiplex, encrypt, encode, and modulate up to four 50 BPS submarine broadcast channels into VLF/LF radio frequency signals that are amplified/radiated by the VLF/LF transmitter antenna.

### **6.23 VERY HIGH FREQUENCY (VHF)**

Very high frequency (VHF) communications, considered by some more as a legacy communications path, still play a major role in day-to-day operations onboard US Navy Ships. Probably the most common use of VHF communications is the Bridge-to-Bridge (BTB) radio. The BTB radio is typically set to monitor channel 16 (The International Maritime Channel); Channel 16 is first commonly recognized as the "distress" channel. Channel 16 will also be used to establish communications and coordinate safety of navigation with other vessels. BTB radios will be monitored at all times underway, at the very least, from the bridge and Combat Direction Center (CDC). Occasionally a scanner will be used in locations such as Radio to monitor BTB as well. Previously, most US Navy BTB radios were militarized radios (e.g. AN/URC-80), however compared to Commercial-Off-The-Shelf (COTS) systems these radios were considered fairly limited. As such, some ships, if not officially outfitted with Commercial-Off-The-Shelf (COTS) systems have purchased radios using their own funds. Functions typically sought after are channel scanning and dual channel monitoring.



### VHF Support for Aviation Communications

VHF communications still play a role in communicating with aircraft and monitoring the International and Military Air Distress (i.e. IAD and MAD respectively) channels. GRC-211 is the radio set commonly associated with this application and has replaced the GRT-21/GR-23 radio suite on several ships.

### VHF Support for Naval Surface Fires Support

Supporting ground forces has always been an integral part of the functions of US Navy ships. For over 30 years ships have maintained the VRC-46 radio as a reliable means of communicating with ground forces. In the last decade, the VRC-46 has been getting replaced by the Single-Channel Ground and Airborne Radio System (SINCGARS). SINCGARS capabilities include:

1. • Provides secure, anti-jam (AJ) VHF voice and data communications in support of amphibious and Naval Surface Fire Support (NSFS) operations
2. • SINCGARS System Improvement Program (SIP) and Advanced Shipboard Improvement Program (ASIP) provide improved data performance at 16 kbps with forward error correction, thus extending range
3. • IP routing and data packet capabilities will be implemented in the SINCGARS interface with ADNS Block 2 (MAGTF Router Upgrade).

## 6.24 BANDWIDTH MANAGEMENT

In computer networking, bandwidth management is the process of measuring and controlling the communications on a network link, to avoid filling the link to capacity or overflowing the link, which would result in network congestion and poor performance.

Anyone who has an Internet connection has at some time downloaded a large file and noticed that the web page starts to load slowly, or fail to load. The reason is that the bandwidth of the internet connection is limited, like the size of a highway, and when someone tries to send too much information down it, more than its capacity, a virtual traffic jam results. This is also known as network congestion.

## 6.25 COMMUNICATIONS CONTROL SHIP (CCS)

Each Strike group is assigned to a Communications Control Ship (CCS), normally an aircraft carrier (CV/CVN) or large deck amphibious ship (LHA/LHD). At a minimum the CCS performs the following functions:

1. At least 72 hours prior to getting underway or executing a shift in the communications plan, promulgate a message to the strike group stating circuit activation priority and times. The CCS tracks the progress of the shift and reports completion to the strike group commander to include circuit status and any problems that may have been encountered during the shift.
2. Act as Net Control Station (NECOS) on all strike group circuits unless otherwise directed by the Officer in Tactical Command (OTC). Each Warfare Commander acts as NECOS on Warfare (Coordination & Reporting) C&R Circuits. The primary responsibility of NECOS is to aggressively manage circuits.
3. Provide missing crypto key, as the designated Over The Air Transfer (OTAT) ship to all ships in the strike group. Perform crypto roll-overs, OTATs and loading.
  - a. The CCS will coordinate daily crypto restarts in accordance with NCTAMS XX2301Z daily message. The CCS will notify all units when to conduct crypto changes.
  - b. The CCS will receive COMSPOT reports from strike group units requiring an OTAT and will identify means of transmission to expedite delivery of the crypto key.

4. Ensure communications circuits are in accordance with the OPTASK COMMS.
5. Monitor all communications outages, casualties, and difficulties within the strike group and offer advice and/or technical assistance as appropriate.
6. Coordinate operation of limited range intercept circuits.
7. Enforce COMSPOT reporting throughout the strike group.
8. Provide ship-shore-ship message traffic relay for strike group units requiring such support in the event of CUDIXS, PCMT and/or Fleet SIPRNET Messaging (FSM)/ADNS casualty.



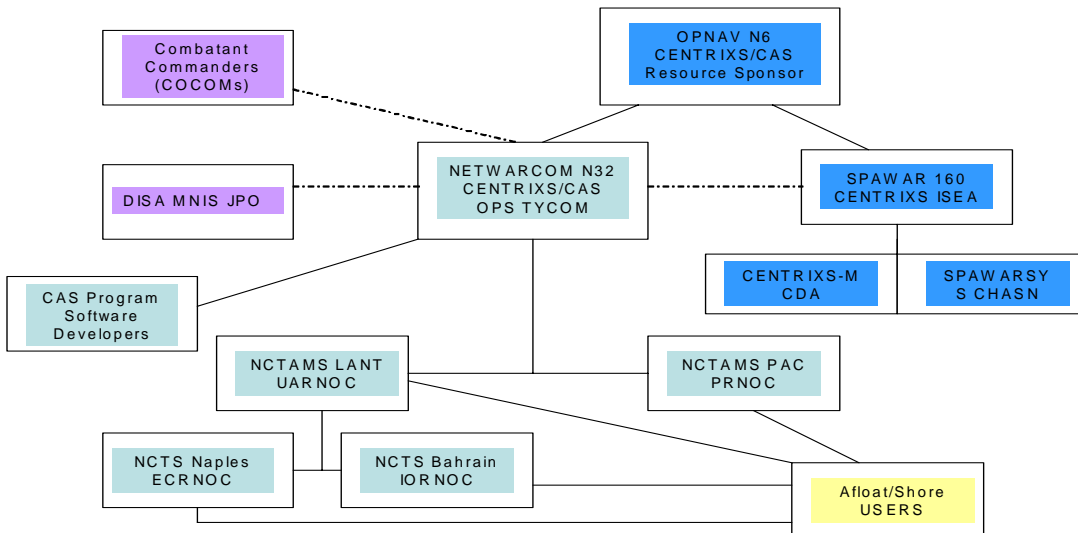
**CHAPTER 7  
ALLIED/COALITION COMMUNICATIONS**

**7.1 CENTRIXS-Maritime**

The CENTRIXS program provides U.S., coalition and allied interests with a secure, reliable, high speed Local Area Network (LAN) with access to the coalition Wide Area Network (WAN). CENTRIXS is a Department of Defense Multi-National Information Sharing (MNIS) program that is resourced by DISA at the COCOM and Joint Military Services level. U.S. Navy, coalition and allied maritime users take part in the CENTRIXS Maritime portion of the global CENTRIXS network. CENTRIXS Maritime or CENTRIXS-M simply refers to the Navy or maritime portion of the global CENTRIXS network.

**7.1.1 NETWARCOM C4 TYCOM**

Naval Network Warfare Command (NNWC) serves as the U.S. Navy C4 TYCOM for all SURFOR, AIRFOR and SUBFOR C4 requirements, and serves as the ISIC to NCTAMS LANT and NCTAMS PAC in the global C4 services, including CENTRIXS and other maritime allied and coalition programs. Additionally, NNWC provides operations direction and oversight for user support for all CENTRIXS (and CAS) shore support at Regional NOCs and subordinate regional nodes, including NMCI and ONE-NET.



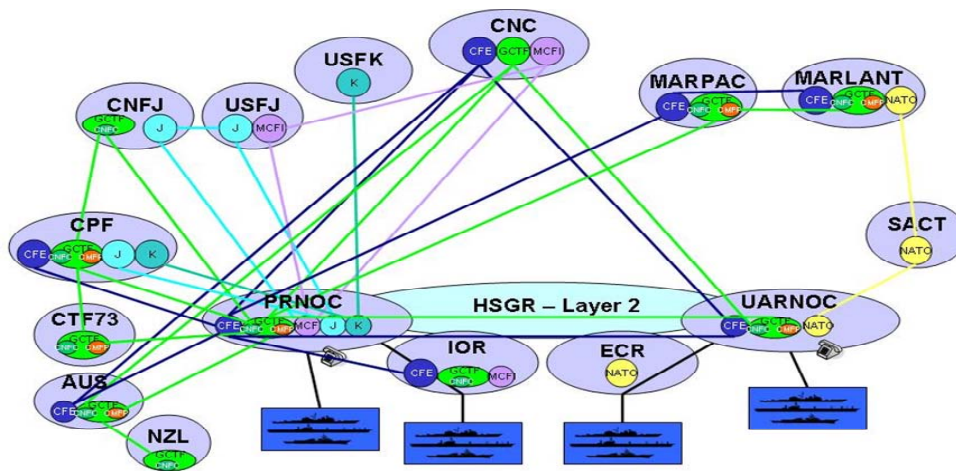
**Figure 7-1  
CENTRIXS-M Organizational Relationships**

**7.1.2 PRNOC CENTRIXS Services**

The Pacific Regional Network Operations Center (PRNOC) or RNOSC West has served as the sole CENTRIXS-M shore service provider since the initial standup of CENTRIXS networks. PRNOC provides CENTRIXS Email, DNS, CHAT, Web, and COP support for all ships and maritime shore users worldwide, and will continue this level of support until UARNOC reaches Initial Operating Capability (IOC) and starts to assume responsibility for its terminated CENTRIXS users. All CENTRIXS enclaves, COI's, and bi-lateral networks will remain operational at PRNOC following UARNOC's CENTRIXS services activation in early FY08.

PRNOC is divided into multiple work centers where SIPRNET, NIPRNET and SCI services remain distinctly separate from CENTRIXS and CAS watch organization. Presently PRNOC CENTRIXS and CAS watch personnel consists of civilian contractors who work day and eve shifts. During mid-watch periods where watch personnel are not present in the PRNOC CENTRIXS watch floor, user requirements are supported by adjacent SIPRNET and NIPRNET watch personnel. Ultimately, the plan is for PRNOC CENTRIXS and CAS OPS to incorporate a 24/7 watch organization.

**Planned Network Connectivity – Phase I**



**Figure 7-2  
CENTRIXS-M Global Connections**

**7.1.3 UARNOC CENTRIXS Services**

UARNOC's CENTRIXS capability was installed in 2007 in support of a planned dual-NOC architecture. UARNOC supports CENTRIXS users that derive their SIPRNET services at UARNOC. Typical supported enclaves include Coalition naval Forces CENTRCOM (CNFC), Combined Maritime Force Pacific (CMFP), Global Counterterrorism Task Force

(GCTF) and the NATO Initial Data Transfer System (NIDTS) networks. UARNOC operates all IP services with a single watch organization. That is, all SIPRNET, NIPRNET, SCI and CENTRIXS services will be managed from a single watch section of primarily military personnel. The watch is presently a 24/7 operation, and deemed to remain 24/7 following the incorporation of CENTRIXS and CAS services.

#### **7.1.4 IORNOC CENTRIXS Services**

The Indian Ocean Regional Network Operations Center (IORNOC) provides a Point of Presence (PoP) for U.S. units operating in the C5F AOR. The PoP was established to provide a more efficient CENTRIXS connection for ships already terminating SIPRNET IP services at IORNOC. Without the PoP, all IP routing for ships in C5F would be sent to PRNOC for access to the CENTRIXS CNFC enclave. IORNOC provides PCHAT, Sametime Services, CAS Replication, Web and limited DNS services. Exchange services are not provided by the IORNOC, e.g. Email - this service is provided by the PRNOC.

COMUSNAVCENT provides GCTF and MCFI full services to U.S. maritime units operating in the C5F AOR. Services provided to designated units include CENTRIXS Flyaway Kits (laptops, router, switch, and TACLANE), which are installed by C5F Fleet Systems Engineering Team (FSET) once the unit has chopped to C5F AOR. Ships are assigned CENTCOM IP addresses, and are given CENTCOM email addresses utilizing the CENTCOM Domains. Services include Email, Web browsing, and MIRC CHAT.

#### **7.1.5 CENTRIXS In-Service Engineering Agent (ISEA)**

The primary function of the CENTRIXS ISEA is to provide technical support of CENTRIXS fielded systems afloat and ashore, including equipment located at PRNOC and UARNOC. Technical support includes installations, network and system engineering, configuration and life cycle management of installed systems. The Shore ISEA works with the CENTRIXS on-site engineers/technicians to provide Tier-4 engineering support. The Tier-4 engineers are normally located at the SSC San Diego Pacific CENTRIXS shore lab facility in Pearl City, Hawaii and the SSC Charleston CENTRIXS shore lab facility in Charleston, South Carolina. The CENTRIXS Central Design Agent (CDA) Shore is also co-located at both east and west coast facilities. The shore ISEA and shore CDA entities will be fully leveraged and will work closely as a team. The expected outcome is improved identification of system requirements and improvement in product development. The Shore ISEA will serve as a feedback loop in the product development cycle to help ensure fielded systems are closely coupled with meeting the Fleet's operational requirements.

### 7.1.6 CENTRIXS Central Design Agent (CDA)

The CDA's primary function is to evaluate requirements, design, develop, test and evaluate, provide cost estimates and deployment timelines (scheduling) in a solutions/capabilities package. The CDA determines the proposed impact to both the afloat (ships) and shore infrastructure (Network Operations Center). The solutions package will then be vetted from the PEO for appropriate acquisition funding. Once funding is obtained, the CDA works with existing entities to provide configuration management control of CENTRIXS for both afloat and shore components is properly followed. The CDA creates the blueprint that Integrated Logistics Support (ILS) used to install the solution at the infrastructure afloat and/or shore. The CDA also maintains configuration control and management of CENTRIXS Maritime.

### 7.1.7 CENTRIXS User

The CENTRIXS User distinction applies to the "organization" that gains access to the CENTRIXS network via a workstation. While numerous options exist to enable CENTRIXS access, the intent of this discussion is to address afloat and shore users, and their roles and responsibilities.

### 7.1.8 Afloat CENTRIXS User

All SURFOR, SUBFOR and AIRFOR ships that have a validated CENTRIXS requirement have been provided a CENTRIXS capability. Installed architectures consist of the following options:

- Block 0 Small combatants with 3-7 workstations and multiple hard drives for several enclave options.
- Block I Flagships/Amphibs/Force-level Ships. Same installation as Block 0, but adds workstations for a total of 15.
- Block II Command Ship/CVN with 30+ multi-level thin clients and access to four enclaves and SIPRNET simultaneously. While Block II enables multiple simultaneous enclave accesses, Block 0/1 will only support one enclave at a time. Swapping out pre-configured hard drives for the various enclaves is required in Block 0/1.

PRNOC also provides services for several allied/coalition ships that terminate directly into the PRNOC. The goal is to have all allied/coalition maritime units derive services from their own country NOC's, and perform only NOC to NOC connections at PRNOC and UARNOC (when operational).

Afloat User Planning: CENTRIXS ISEA (SPAWAR) provides post installation training, however, on demand or follow up training for Afloat units is provided by NNWC funded CENTRIXS Global

Support Team (GST). Afloat commands that have not operated CENTRIXS systems for extended periods (between deployment cycles) can request refresher training through the CENTRIXS GST. Ships are also responsible for ensuring that CENTRIXS hard drives (Block 0/1) are onboard for network requirements. Multiple hard drives are provided based on operational requirements at time of installation. However, if/when requirements change, coordination with SPAWAR CENTRIXS ISEA is necessary to ensure required CENTRIXS enclaves can be accessed. Contact SPAWAR Fleet Support Desk (FSD) for coordination.

#### **7.1.9 Shore CENTRIXS User Access**

Shore commands that have a requirement for access to CENTRIXS must coordinate CENTRIXS network access with the applicable supporting RNOSC (NOC). The NOC watchstander will refer the requesting station to download the applicable MOA template from the NOC website. This MOA will spell out the responsibilities of both user and supporting NOC. Once the MOA and approved IATO/ATO is received by the supporting NOC the coordinated effort of network access establishment will begin. CENTRIXS services will typically be provided by the same NOC that provides SIPRNET and NIPRNET services. Coordination for CENTRIXS network access should be coordinated 30 days prior to desired network activation, but no earlier than 10 days.

#### **7.1.10 CENTRIXS IA/CND Responsibilities**

CENTRIXS Computer Network Defense (CND) policies have not yet been established by the JTF GNO or NCDOC. In the interim, a multi-national working group, comprised of the NETWARCOM led Maritime Multi-National IP Interoperability (M2I2) Steering Group IA leads, has mutually developed a Maritime CENTRIXS CND Standard Operating Procedure (SOP) to be used by all CENTRIXS Maritime users. This CND SOP will aide with providing guidance for reporting CND incidents, and minimum protection requirements of network resources.

The CND SOP noted above is available for download via the NCTAMS PAC SIPRNET web site at: [www.nctamspac.navy.smil.mil](http://www.nctamspac.navy.smil.mil). Once in the site refer to the Allied/Coalition link.

#### **7.1.11 CENTRIXS/CAS Help Desk Responsibilities**

CENTRIXS Help Desk functions are managed at several different levels. PRNOC and UARNOC manage a Help Desks that deals with user configuration, performance and general operations issues. SPAWARSYSCEN San Diego Code 2631 also manages a CENTRIXS Help Desk role within the Fleet Support Desk (FSD). The FSD Help Desk responds to Program of Record related to software, hardware, logistics, training, documentation, and various other technical assistance issues that are beyond the typical watch personnel capability at PRNOC to resolve.

NOC Help Desk: users experiencing difficulties with CENTRIXS enclaves, including software, hardware or configurations will contact the Help Desk for troubleshooting and assistance. The NOCs also manage a CAS Help Desk, co-located at the NOC watch floor. Users will contact the appropriate NOC (PRNOC/UARNOC) where their CENTRIXS (or SIPRNET/NIPRNET) services terminate. This means that servicing NOCs that provide SIPRNET services will also provide CENTRIXS Help Desk support for the same command/user. Making contact with the NOC Help Desk can be accomplished via telephone, email, COMSPOT or CHAT session. Refer to appropriate CIB/CIA's for policy/procedures for obtaining Help Desk support. Refer to GCIB 3B for detailed guidance for reporting guidance, and IP address information for the various services.

### 7.2 Global CENTRIXS Network

Figure 7-3 below displays a snapshot of existing user commands that receive CENTRIXS and/or CAS services from PRNOC. With the ever-changing environment of CENTRIXS operations, it would be very difficult to capture all partner nations and services that are derived from U.S. Navy NOCs. For example - today, several coordination talks are underway between NETWARCOM, COCOMs and allied nations who desire to be added to existing CENTRIXS enclaves. For this reason it would be impractical to capture all global connections.

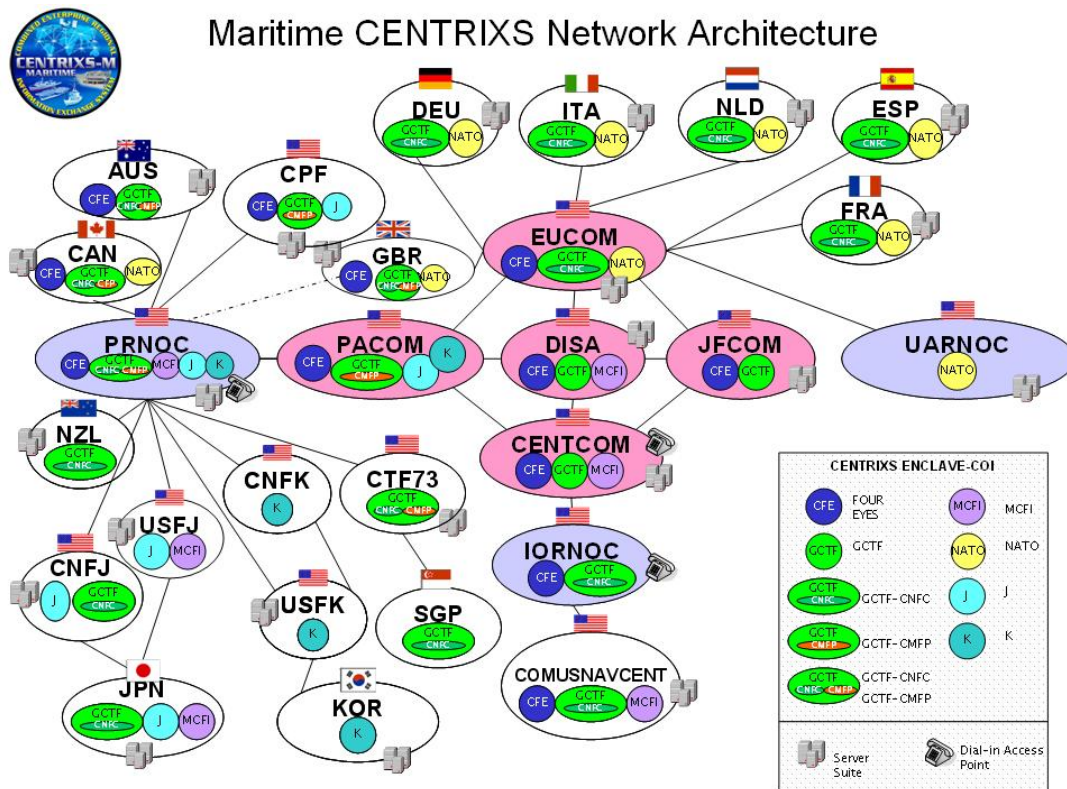


Figure 7-3  
Current CENTRIXS Architecture (single NOC)

### 7.2.1 CENTRIXS Enclaves

The global CENTRIXS network consists of numerous individual enclaves that are cryptographically separated based on access and releasability. U.S. CENTRIXS users utilize SIPRNET for transport of CENTRIXS networks via KIV-7, KG-175, KG-84 or comparable Type 1 encryption devices. A discussion about each of the CENTRIXS enclaves is provided later in this chapter. The following CENTRIXS enclaves are available based on requirements: CENTRIXS Four Eyes (CFE), GCTF and MCFI. Communities of Interest (COI) include: CMFP and CNFC. Bi-lateral networks include: CENTRIXS K, which supports bi-lateral operations with South Korea and the United States, and CENTRIXS J, which supports bilateral operations between Japan and the United States. Global Counterterrorism Task Force (GCTF) exists for combined operations with the countries supporting the Global War on Terrorism. NATO Initial Data Transfer System (NITDS) supports combined operations between NATO allies. Note: While NATO takes part in coalition operations/exercises, the distinction is that NATO sets policies for NATO networks; Combatant Commanders, e.g. CENTCOM, PACOM, etc., sets policies for CENTRIXS.

Each enclave has specific capabilities but common to each are:

1. The ability to send and receive Email
2. Web browsing
3. Web site replications via CAS
4. CHAT
5. CHAT with logging (Persistent CHAT)

### 7.2.2 CENTRIXS Four Eyes (CFE)

CFE represents an end-to-end data network architecture to share SECRET and below releasable information for combined operations with members of Australia, Canada, United Kingdom, and the United States (AUSCANUKUS). System elements include web services, e-mail, chat, COP, Domain Name resolution, network routing, access, and access control.

### 7.2.3 Global Counter-Terrorism Task Force (GCTF)

The GCTF enclave includes those countries currently supporting the Global War on Terrorism. Most ships deploying to C5F, C6F, or C7F do not receive GCTF as one of the available enclaves, however, some BLK II (CVN/LCC) platforms have received GCTF based on having the capacity to manage four (4) simultaneous enclaves. At the time of this document development more than 60 nations are taking part in GCTF in the global war on terror. USN ships that require GCTF must provide ample time before deploying to enable SPAWAR engineers to build GCTF hard drives (if required).

#### **7.2.4 Multi-Coalition Forces Iraq (MCFI)**

The CENTRIXS MCFI is essentially a separate enclave that is used only within the CENTCOM AOR. MCFI is typically used by shore ground forces (non-maritime). USN ships are not typically required to take part in the MCFI network. An MCFI user is not supporting a maritime role.

#### **7.2.5 GCTF Communities of Interest (COI)**

A COI is defined as a collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange.

The Community level is similar to the enclave level as it provides customized services based on user requirements for unique applications or services that may include specialized firewalls, virtual private networks, intrusion detection, proxy and content checking services. Allies must tunnel through a VPN concentrator to enter the CNFC network. U.S. ships are within the boundaries of the CNFC network and behind the CNFC VPN concentrator as SOP. U.S. ships can access GCTF only by prior coordination with the PRNOC. If they need to access GCTF then the PRNOC personnel have to make configuration modifications at their equipment.

There are very significant differences between GCTF COI's and CFE, for example:

1. E-mail - cross-enclave e-mail is not permitted; COI emails may only be sent to other COI users within the same physical COI.
2. Collaboration At Sea (CAS) - U.S. users may not release information from the SIPRNET CAS to a GCTF, COI or bi-lateral web sites.

#### **7.2.6 Combined Naval Forces CENTCOM (CNFC)**

Allied forces in the Central Command (CENTCOM) AOR rely upon and act in collaboration with coalition partners in pursuit of national security objectives. The Commander, U.S. Navy Central Command (CUSNC) has directed that the Global Counter Terrorism Force (GCTF) enclave of the CENTRIXS is the network of choice for maritime coordination throughout the CENTCOM AOR. CENTRIXS CNFC is used for tactical level coordination between coalition nations and forces operating as part of the CFMCC task organization. COMUSNAVCENT has directed that all coalition ships and units deployed to the C5F AOR to support CFMCC operations are operating within the CNFC network.



### **7.2.7 Cooperative Maritime Forces Pacific (CMFP)**

CMFP was developed by COMPACFLT out of need to have a CENTRIXS enclave in the Pacific to be used during multi-national exercises in the Pacific RIM. While CMFP has not been used (as of this date) in GWOT operations, the CMFP network is envisioned to be used in future operational scenarios to support Pacific area real world allied/coalition requirements.

### **7.2.8 Bi-Lateral Networks**

The ultimate goal of all bi-lateral networks is to have full redundancy at both regional NOCs. Initially, however, the CENTRIXS-K/J networks will continue to be managed exclusively by the Pacific Regional NOC in Wahiawa, HI. As resources and funding is made available bi-lateral networks will be fully redundant at both NOCs. Until such time that Cross-Domain Solutions will enable access to multiple security domains, the numerous CENTRIXS enclaves, and bi-lateral networks will require individual access/routing and security to limit exposure and access by undesignated allies/coalition partner nations.

### **7.2.9 CENTRIXS-Korea (CENTRIXS-K)**

CENTRIXS-K is a U.S. Forces Korea managed network (formerly GCCS-K) that is supported exclusively at the PRNOC for U.S. Navy maritime requirements/users. While CENTRIXS-K can be extended worldwide via IP routing, anticipated use of CENTRIXS-K is limited to the Pacific and Indian Ocean operating areas, and thus will not be initially installed at UARNOC.

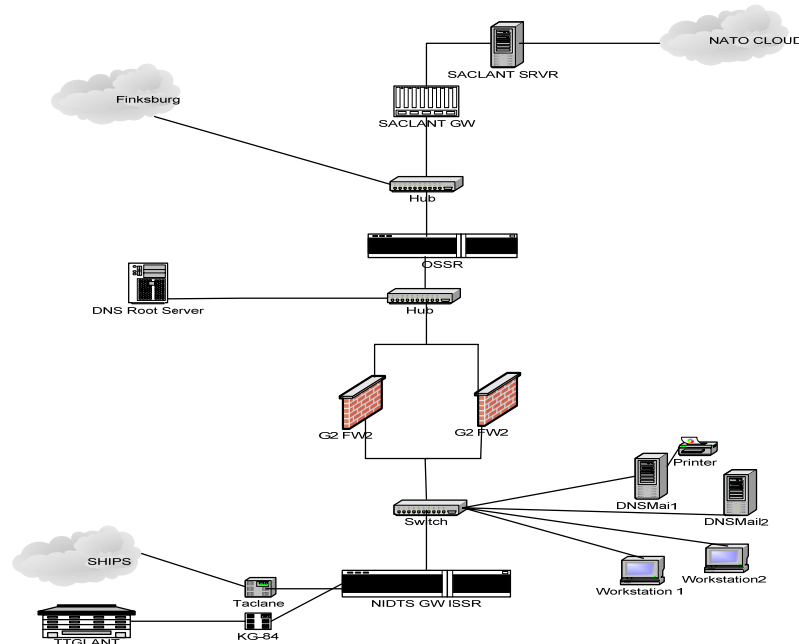
### **7.2.10 CENTRIXS-Japan (CENTRIXS-J)**

CENTRIXS-J is a U.S. Forces Japan managed network (formerly the bi-lateral wide area network BWAN)) supported by the PRNOC. As noted with CENTRIXS-K, this network will also initially be managed exclusively by PRNOC for all users/requirements.

## **7.3 NATO Initial Data Transfer System (NIDTS)**

The UARNOC serves as the sole U.S. Navy NOC to provide NIDTS/NATO Secret (NSWAN) access to the NATO C4 network. While NIDTS' architecture is very similar to that of CENTRIXS enclaves, the visibility and access only by NATO partner nations makes its use unique and dissimilar to CENTRIXS. Additionally, NIDTS is managed by SHAPE and subordinate NATO commands. Numerous connections exist within the United States to NIDTS, however, only those maritime NIDTS connections that support shipboard users are managed by the UARNOC in Norfolk, VA. NIDTS can be accessed with the same equipment infrastructure used aboard CENTRIXS configured ships by using a NIDTS hard drive and slight IP routing configurations. For new NIDTS requirements contact UARNOC personnel for details. There is currently no plan to

provide the same dual NOC redundancy for NIDTS as for the other CENTRIXS enclaves. Future plans will call for an alternate site for NIDTS, however, specific details have not yet been established.



**Figure 7-4**  
**NATO Initial Data Transfer System (basic architecture)**

### 7.3.1 NIDTS Connection Requirements

UARNOC receives a NIDTS Service Request Transmission Summary (SRTS) order for U.S. ships from NCSA HQ Brussels. From that message UARNOC utilizes the LAN and WAN IP addresses provided in the message to configure a tunnel within the inner router to the unit/command. The ship must provide UARNOC their tunnel source and the IP address of the ship's exchange server. UARNOC hosts internal and external DNS for all U.S. ships via domain "usn.nato.int." for external and "shipname.usn.nato.int for internal." UARNOC configures SMTP connections for all U.S. ships for email exchange. UARNOC receives the NATO GAL from SACT-ASP via directory replication. UARNOC and U.S. ships use JEDR for exchange of the NATO GAL. UARNOC configures the NIDTS firewall from requests submitted by U.S. ships.

Re-establishing existing inactive NIDTS networks. Ships that have not been active on their NIDTS network connections for extended periods require reloading current cryptographic keymat/keys in the COMSEC device, load the hard drive into the server (if applicable), and download a current Global Address List (GAL). Contact the supporting NOC for coordination and guidance.

NIDTS services provided by UARNOC are limited to 24X7 Email and web browsing.

**7.4 Battle Force Electronic Mail 66 (BF EMAIL)**

Background: Battle Force E-Mail 66 (BFEM 66) is a program evolved from the requirements of the High Frequency Data System ORD. Battle Force E-Mail emerged in the early 1990's as a low level development and integration effort to validate IP based connectivity in the HF environment. In the late 1990's, the generation of STANAG 5066 for HF Data Profiling coupled with the availability of higher speed HF modems and the COTS implementation of the STANAG 5066 waveform for email exchanges made BFEM 66 a viable candidate for implementation in support of Allied interoperability. Battle Force E-Mail 66 provides a basic inter-ship user-to-user IP secure data transfer capability between U.S. strike groups and allied, NATO, and Coalition afloat forces via standard HF radios with KG-84A/C generated encryption.

**7.4.1 BFEM Configuration**

For setup of BFEM hardware for operational use consult the NCTAMS Allied Networks link to obtain the Standard Operating Procedure (SOP). This SPAWAR developed SOP provides configuration and equipment setup procedures. If additional assistance is required contact SPAWAR Charleston via contact information located in para 7.4.2 below.

**7.4.2 BFEM Technical Support**

SPAWARSYSCEN Charleston has been designated as the ISEA and provides remote and onsite shipboard hardware technical support for BFEM 66. All requests for technical support should be directed to the ISEA via the SPAWARSCOM Help Desk as follows:

Phone Number	E-mail Address	SIPRNET Address
(877) 4-SPAWAR	<a href="mailto:CCSPAWAR@SPAWAR.NAVY.MIL">CCSPAWAR@SPAWAR.NAVY.MIL</a>	<a href="mailto:CCSPAWAR@SPAWAR.CHAS.NAVY.SMIL.MIL">CCSPAWAR@SPAWAR.CHAS.NAVY.SMIL.MIL</a>

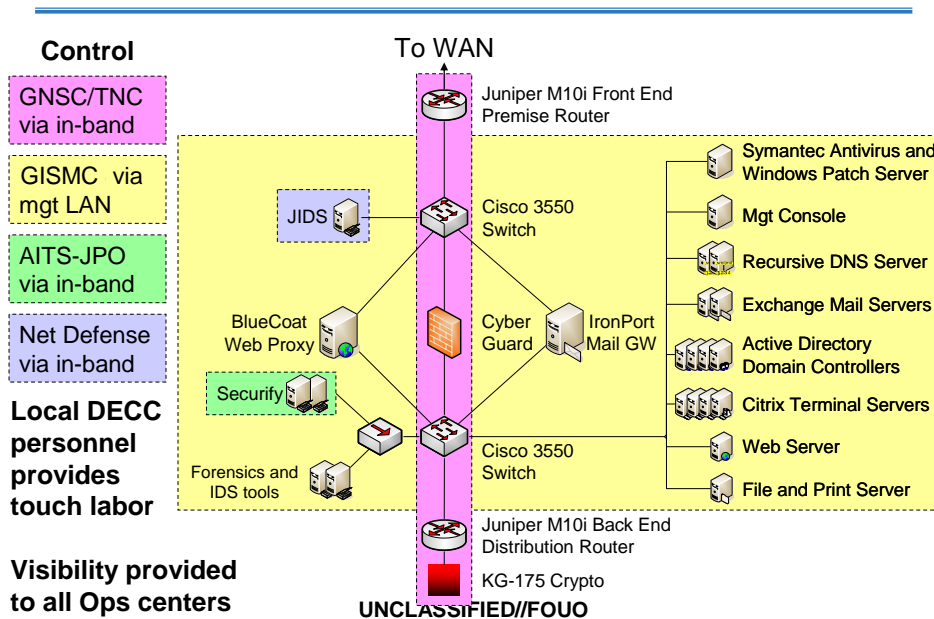
**7.5 Common SIPRNET Domain (CSD)**

Background: The REL Network or "DMZ" provides several services that enable information sharing between US Users and foreign national/exchange officers embedded in US enclaves and in enclaves located in partner countries. There are two primary REL user types: In-Country and Embed. In-Country users are located in a partner country enclave (a physical location owned and operated by the partner country) and are directly connected to the REL DMZ through their locally managed REL Enclave. Embed users are physically located within a US CCSA (physical location

owned and operated by the US) and connect to the REL DMZ through GRE tunnels from the locally managed US CCSA. From a user perspective, using the REL Network and the REL DMZ and its associated services closely mirrors a typical Windows enterprise environment. Users will be provided standard Windows applications/services such as a web browser, email client, office applications, and file server access. See Table 2 for a more complete listing of applications/services and the organization that is responsible for providing them.

Two areas in which the user experience will differ from a typical Windows experience are web access and email. Web Access through the REL DMZ requires all web traffic to pass through a web proxy and to be scanned by a content filter. These mechanisms help secure SIPRNet resources that have been deemed non-releasable. For each browser session, the first attempt to access web content will require the user to authenticate to the web proxy. Embedded users will be presented with a dialog box similar to Figure 1 in order to enter the authentication information. In-Country users will not see this dialog box. If you are embedded and you do not receive this dialog box when accessing web content for the first time, contact your local administrator immediately.

### DMZ Architecture



**Figure 7-5**  
**Common SIPRNET Domain**

Email differs from a typical Windows enterprise environment in that there are specific requirements for mail to be delivered as well as criteria that will reject email delivery under most circumstances. For email to be considered for delivery it must contain a CAPCO marking that marks the email content as releasable to coalition partners. CAPCO Releasable markings are

found in Table 7-1. Email with an appropriate CAPCO marking will be delivered unless the body of the email or any attachment contains the term "NOFORN". This term indicates the content is not releasable to foreign nationals and will therefore be rejected by the mail filter. It is possible to send NOFORN-designated information via the REL DMZ with the use of a positive marking statement. This statement will allow otherwise rejected content to be delivered because the sender is certifying the content is releasable to all parties. Contact your local administrator if you feel you have a need to use the positive marking filter.

<b>CAPCO Classification Markings</b>	
Unclassified	SECRET//REL TO USA, ACGU
Unclassified//FOUO	SECRET//REL TO USA and AUS
CONFIDENTIAL//REL TO USA and GBR	SECRET//REL TO USA and CAN
CONFIDENTIAL//REL TO USA and AUS	SECRET//REL TO USA and GBR
CONFIDENTIAL//REL TO USA and CAN	SECRET//REL TO USA, AUS and GBR
CONFIDENTIAL//REL TO USA, AUS and GBR	SECRET//REL TO USA, AUS, CAN and GBR
CONFIDENTIAL//REL TO USA, AUS, CAN and GB	R

**Table 7-1**  
**CAPCO Classification Markings**

### User Information

Embed users will have two (2) separate accounts: one (1) for the REL DMZ and one (1) for their local CCSA. The REL DMZ account will be used for web access only. The CCSA account will be used for accessing all other services. Non-embed users will use their REL DMZ account to access all services.

Table 7-2 provides a breakdown of the various user types, their login and email domains, as well as their primary support contact. The "Expectations" section further defines the group responsible for providing various services and the support contact for these services for each user type.

User Type	Login Domain*	Email Domain	Main Support Contact
In-Country (GBR, AUS)	DMZ**	dmz.rel.smil.mil	CNC (GBR) Local Admin (AUS)
In-Country (CAN)	CAN	can.rel.smil.mil	Local Administrator
Embed (GBR, AUS, CAN)	Local domain (e.g. DISA)	Site specific email (e.g., disa.mil)	Local Administrator
Thin-Client Users (GBR)	DMZ (via Citrix)	dmz.rel.smil.mil	CNC

\* Contact your local administrator for help logging in to the correct domain

\*\* DMZ domain passwords can be changed at [www.dmz.rel.smil.mil](http://www.dmz.rel.smil.mil). All other domains should contact their local administrator for assistance

**Table 7-2  
User Information**

All user types will have a REL DMZ account. As a result, embed users will have two (2) separate accounts: one (1) for the REL DMZ and one (1) for their local CCSA. The REL DMZ account will be used for web access only. The CCSA account will be used for accessing all other services. Non-embed users will use their REL DMZ account to access all services.

- **Expectations**

REL Users should expect a core set of services available for their use at all times. These services include access to office applications, an email client, a web browser, network file shares, an email account, and SIPRNet web sites. The provider(s) of each service, and support of the service, is dependent on the user type. This section identifies the provider and support contact for each service by user type.

#### *In-Country (GBR, AUS) Users*

All core services except an email account and SIPRNet web access are provided by the local In-Country enclave. Email accounts and SIPRNet web access will be provided by the REL DMZ. Embed users can change their REL DMZ password online at <http://www.dmz.rel.smil.mil> or by using normal Windows procedures. Users should contact the Coalition NetOps Center (CNC) if it is necessary to reset their password or if they experience issues accessing SIPRNet web sites. All other issues should be directed to an In-Country administrator.

#### *In-Country (CAN) Users*

All core services except SIPRNet web access are provided by the local In-Country enclave. SIPRNet web access will be provided by the REL DMZ once a DD2875 form has been received and approved by the CNC. Users should contact the CNC for issues accessing SIPRNet web content. Users will be able to change their REL DMZ

password using normal Windows procedures or by contacting an In-Country enclave administrator for help. All other issues, including password resets, should be directed to an In-Country administrator.

#### *Embed (GBR, AUS, CAN) Users*

All core services except SIPRNet web access are provided by the local CCSA. SIPRNet web access will be provided by the REL DMZ. Users should contact the CNC for issues accessing SIPRNet web sites. Embed users can change their REL DMZ password. Users can change their REL DMZ password online at <http://www.dmz.rel.smil.mil>. Changing the Windows logon password can be achieved through Windows or by contacting a CCSA administrator. Users should contact the CNC for REL DMZ password resets and a CCSA administrator for Windows password resets. All other issues should be directed to a CCSA administrator.

## **7.6 GRIFFIN**

The Griffin Combined Wide Area Network (CWAN) is a classified electronic information-sharing environment for collaborative planning activities between strategic, operational and tactical level headquarters. Griffin provides a means for dissemination of information between participating nations for planning, implementing and executing multinational operations. For specific issues concerning releasability and coalition partners operating on Griffin, browse to: <http://rela.griffin.disa.smil.mil>

Prior to requesting individual Command specific account, Commands coordinate with Griffin Community Manager to establish a Command Training Verification POC. User tutorials and foreign disclosure training available are on the Griffin website to assist users in getting started. Griffin users must be acutely aware of limitations of the Griffin mail guards, and specifically, trained on disclosure issues.

### **7.6.1 GRIFFIN Account Setup**

1. Take Griffin Training online at Griffin website.
2. Notify Training Verification POC with Directory Contact information: First Name, Last Name, Rank, Role, Country, SIPRNET E-mail, and Phone Number.
3. All account information submitted by POC to Griffin by Tuesday COB will have accounts ready by Friday of the same week. Account information received after Tuesday COB will be in the next week's implementation.
4. When your account is ready, start sending Griffin E-mails from your regular SIPRNET Inbox.

### **7.7 High Frequency Internet Protocol (HFIP) Networking with Coalition Partners**

See Chapter 5 for HFIP discussion. Note: While HFIP is utilized in a coalition environment, its architecture, setup and procedures are comparable in both SIPRNET and CENTRIXS environments.

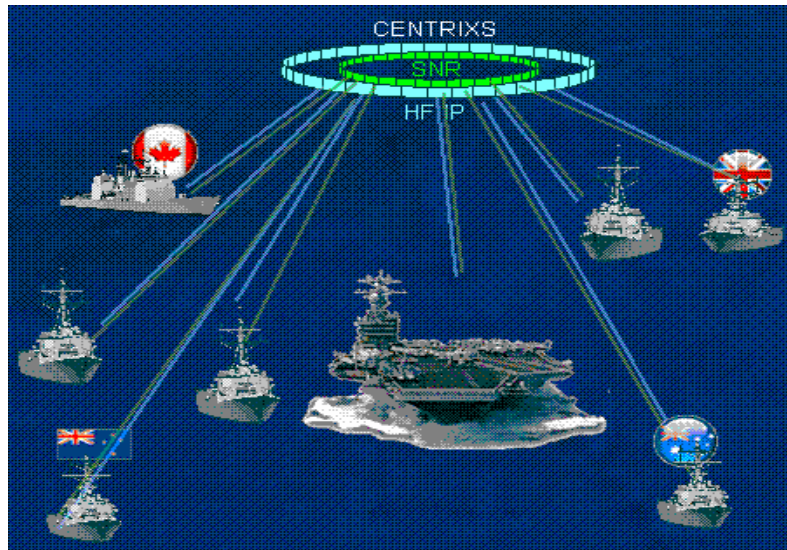
### **7.8 UHF LOS Subnet Relay (SNR) with Coalition Partners / Line of Sight and Beyond Line of Sight Networking with Coalition Partners**

Line of Sight (LOS) and Beyond Line of Sight (BLOS) networking with Coalition partners is being introduced on CENTRIXS via Ultra High Frequency (UHF) Sub-Network Relay (SNR) and High Frequency Internet Protocol (HF IP) systems as added Radio Frequency (RF) bearers. HFIP and SNR are Global Maritime Partnership Initiative programs that enable US ships to communicate up to normal HF and UHF ranges in a tactical environment using CENTRIXS and enabling interoperability in coalition and multinational operations such as Anti-Surface Warfare, Maritime Interdiction Operations, Humanitarian Assistance/Disaster Relief, Global War on Terror and Major Combat Operations. In addition to SATCOM, CENTRIXS networks will now employ LOS/BLOS networking systems such as UHF SNR and HFIP.

### **7.9 High Frequency Internet Protocol (HFIP) and Sub-Network Relay (SNR)**

HFIP and SNR provide Allied, Coalition and US maritime units with a direct platform-to-platform tactical networking capability using standard UHF and HF voice radios with KG-84A/C generated bulk encryption for Transmission Security (TRANSEC). Since the two technologies operate efficiently with current legacy equipment, they are cost effective solutions for achieving tactical IP networking at sea. HFIP and SNR enable war fighters on Combined Enterprise Regional Information Exchange System-Maritime (CENTRIXS-M) to plan and execute coalition operations in a real-time tactical environment by transporting IP data directly to and from ships. HFIP operates in the HF spectrum capable of data rates of 9.6 Kbps in single side band (SSB) and 19.2 kbps in independent side band (ISB). SNR operates in the UHF spectrum capable of data rates up to 96 Kbps. Both systems give surface platforms the ability to share a single SATCOM resource for reach back capability. HFIP also supports the hardware/software upgrade requirements for Battle Force Email (BFEM 66) and is designed to be backwards compatible with BFEM 66. Figure 7-6 is an Operational View of HFIP and SNR.





**Figure 7-6**  
**HFIP and SNR OV-1**

### Status

Based upon an emergent fleet requirement to accelerate fielding, Assistant Secretary of the Navy, Research Development and Acquisition (ASN RD&A) designated HFIP and SNR as a Rapid Deployment Capability. In 2007, HARRY S TRUMAN was the first Strike Group to deploy with HFIP and SNR. Two more Strike Groups are planned to deploy in 2008 with HFIP and SNR. Over the next six years the Navy plans to install HFIP and SNR on approximately 180 ships.

### Developers

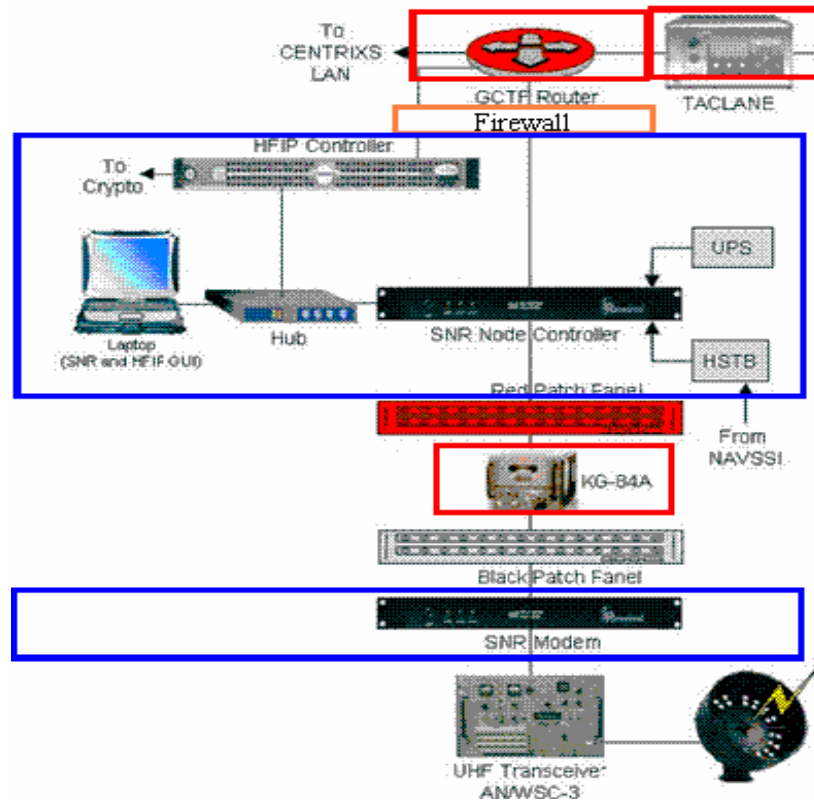
HFIP and SNR projects have distinct technical development and sponsorship, but both address the same requirement: the transport of IP data using existing tactical LOS and BLOS bearers. Australia, Canada, New Zealand, United Kingdom and United States (AUSCANNZUKUS) started the SNR project in 2000, with OPNAV support in the United States to add an IP data transport capability to tactical voice circuits. The resulting design was optimized for UHF/VHF and the first SNR sea trial was in 2003. The HFIP project was started in 2002, with the Office of Naval Research (ONR) support, to add a full IP capability and robust multi-member networking to the Battle Force Email system using HF. HFIP conducted its first trial in 2002. More recently, both systems have been the basis of AUSCANNZUKUS initiatives during Trident Warrior 05, 06 and 07. Hardware for procurement and development of both HFIP and SNR are now under the cognizance of PEO C4I PMW/A-170, OPNAV N6 and NNWC.

### HFIP Overview

The HF IP controller implements an IP client, a BFEM 66 backwards compatible mode, a wireless token ring channel access scheme (to support multi-platform networking) and a STANAG 5066 Automatic Repeat Request (ARQ) engine. The HF IP system is designed to be used in conjunction with the MIL-STD-188-110B HF modems employed by the BFEM 66 system. These modems burst at rates up to 9.6 kbps in Single Sideband (SSB) and 19.2 kbps in Independent Sideband (ISB). HF IP is designed to employ the BFEM 66 HF shipboard infrastructure. This typically consists of a Harris RF5710A modem, a KG-84C crypto and HF transmitter, receiver, couplers and antennas. HF IP brings one new piece of equipment: the HFIP network controller. HFIP was designed to use HF ground wave propagation in order to achieve maximum throughput on HF. HF ground wave propagation distances are specific to a given environment and transmit power, but surface ranges up to 150nm can be expected.

### SNR Overview

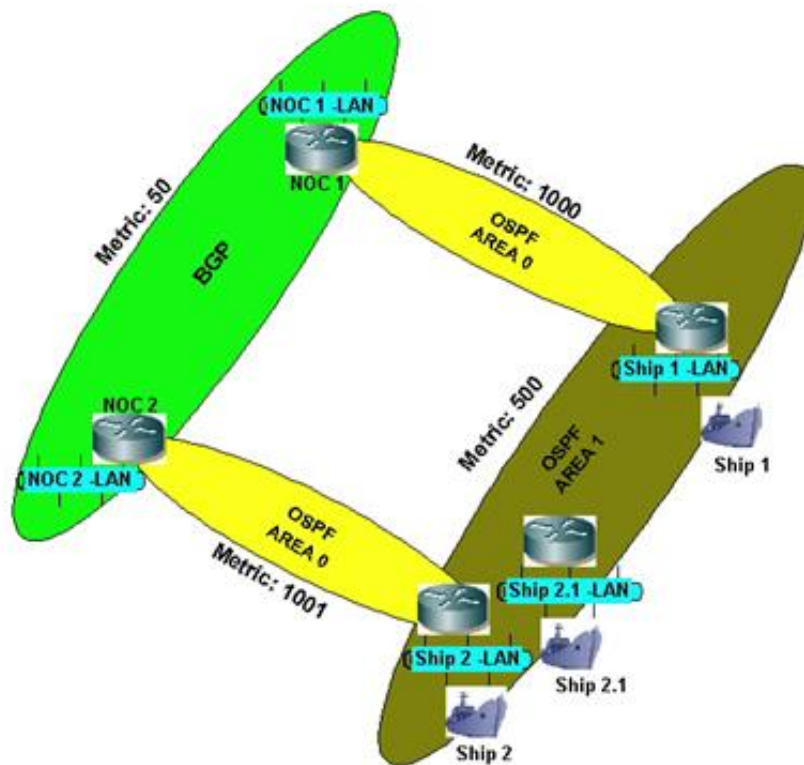
A typical SNR configuration would employ AN/WSC-3 UHF transceiver, couplers and antenna, and KG-84A or KIV-7. UHF SNR brings two new pieces of equipment: an SNR node controller and an external, high speed UHF modem. The UHF SNR controller implements a synchronous Time Division Multiple Access (TDMA) channel access scheme to coordinate on-air transmissions between multiple platforms, optional Automatic Repeat Requests (ARQ) for retransmission of dropped data frames, and automatic traffic relay to forward traffic in the event of multi-hop topologies. The SNR subnet presents itself as a "cloud" to the attached router with the details and dynamics of the underlying connectivity. The SNR modem employs a multi-waveform concept, supporting a range of data rates up to 96 Kbps. UHF SNR LOS propagation depends largely upon the height of the UHF antennas above the waterline. Maximum surface ranges up to 20nm can be expected. SNR also provides for the automated relay of IP traffic to nodes beyond the origination node's radio horizon. For example, Ship A may have traffic destined for ship C, which is 35nm away. Ship B is able to see both ship A and Ship C. Ship A is able to send IP traffic to ship C, via automatic relay at Ship B. SNR supports up to 4 relays, providing a nominal reach of 80nm if ship relay platforms are available. Airborne relays would extend this relay reach considerably. Figure 7-7 illustrates a System View of SNR.



**Figure 7-7**  
**SNR System View**

### Line of Sight Routing Architecture Overview

With HFIP and SNR providing Line of Sight networking with Coalition, a discussion of the LOS networking architecture is in order, as these are new technologies. HFIP and SNR provide mobile ad hoc networking capability. CENTRIXS makes use of this capability via dynamic routing over SNR and HFIP. This is accomplished by implementing multiple Open Shortest Path First (OSPF) Areas at sea and in running Border Gateway Protocol (BGP) between the national NOCs. The router configurations are maintained by their National NOCs and be well coordinated with the CENTRIXS PRNOC. Figure 7-8 illustrates this routing architecture.



**Figure 7-8**  
**CENTRIXS LOS/ELOS Routing Architecture**

On the ships, SATCOM links are assigned to OSPF Area 0 and the LOS/ELOS links are assigned to OSPF Area 1. UHF SNR is assigned a lower link cost than HF IP, since it supports higher bandwidth. Ship Local Area Networks (LANs) are statically routed and "area-less". Router-to-router traffic is filtered to free up bandwidth for operator applications. The ship and NOC routers are configured so that ship-to-shore traffic will be routed to the closest shore node. From this node, traffic is then routed to its destination using terrestrial assets, such as NOC-NOC links.

All shore-to-ship traffic is routed via the national NOC of the destination ship, whenever that ship has a direct SATCOM connection. Shore-to-ship traffic will fail over to another national NOC only when direct SATCOM is down, and another nation's ship could reach the destination ship over the LOS/ELOS bearers.

BGP weights are also employed to direct traffic destined for one nation's ships to its national NOC when that NOC advertises the ship. In the PRNOC routing configuration, a BGP weight of 40,000 is assigned to simulated Coalition ship routes when learned from a Coalition NOC. The default BGP weights are 0 when learned from a BGP neighbor and 32,768 when self-injected. BGP prefers higher

weights, so the path to the Coalition ship via the Coalition NOC is preferred if present.

If the direct SATCOM link between a national NOC and one of its ships fails, BGP will failover to a route via another nation's NOC, if one exists and there is no alternative path within the national Autonomous System (AS). If the direct SATCOM link recovers however, BGP will normally continue to prefer the path via the other nation's NOC, since the ship is now regarded by BGP as belonging to the other nation's AS. In order to insure that routing is always via the direct national connection when available, conditional BGP advertisements are used. This is accomplished using "advertise" maps and "non-exist" maps, keying off the presence or absence of the SATCOM links in the BGP database. One such entry will be required for each allied ship. These statements eliminate the allied ship routes when the allied SATCOM link recovers after a failure.

Finally, Autonomous System (AS) "prepending" is employed when each national NOC injects routes learned from another nation's ships (through OSPF) into BGP. This is done so that external traffic will be preferentially routed directly to the appropriate national NOC whenever that NOC advertises that it can reach its own ships.

#### Operational and Technical Support

As UHF SNR and HFIP are newly introduced technologies, documenting the network configuration of those ships and Strike Groups so equipped is essential to ensure proper operation, configuration control and support. Allied Communications Publication 200 (ACP 200) defines such a document, the OPTASK NET. Within the OPTASK NET, detailed network configurations and points of contact are delineated.

LOS networking offers the possibility of direct ship-ship communications. To date, SOPs have been developed permitting ship-ship DNS services, Exchange E-mail and C2PC Gateway traffic if HFIP or SNR connections are available. If a Sametime chat server is available on a Force Level ship, it is also possible to utilize the Sametime Connect Client with the Force-Level ship server in a ship-ship mode in the event of satellite outage.

In the event of SATCOM outage, and no Sametime server is available afloat, the ship-ship connectivity permits units to reach back to shore via another ship. HFIP or SNR will relay IP traffic to a platform with SATCOM connectivity, allowing the affected unit to reach shore services at the NOC and beyond.

#### **7.10 AUSCANNZUKUS Background**

Early in WW II the lack of communications interoperability between Allied Forces became a matter of concern for all nations.

During 1941 the first high level proposals to formally structure combined operations between the US and United Kingdom was considered. These discussions were the genesis of the current Combined Communications Electronic Board (CCEB). The origins of the AUSCANNZUKUS organization arose from dialogue between Admiral Burke and Admiral Lord Mountbatten, in 1960. AUSCANNZUKUS strategies are to establish C4 policy and standards; identify interoperability requirements and risks; developing and utilizing new technologies and exchanging information on national C4 capabilities, plans and projects. OPNAV N6, OPNAV N6F4, SPAWAR 05 and SPAWAR Systems Center San Diego chair and represent the US at the various AUSCANNZUKUS conferences and working groups. OPNAV N6F4, SPAWAR 05, and SSC SD work together to support the HFIP and SNR Program Office PMW-170 and In-Service Engineering Agent to ensure Strike Groups and coalition nations deploy with the proper operation, configuration control and necessary support. AUSCANNZUKUS, SPAWAR 05, SPAWAR Systems Center San Diego and the ISEA will assist the Strike Group Commander in generating the OPTASK NET. Figure 7-9 illustrates AUSCANNZUKUS interaction with other interoperability groups.

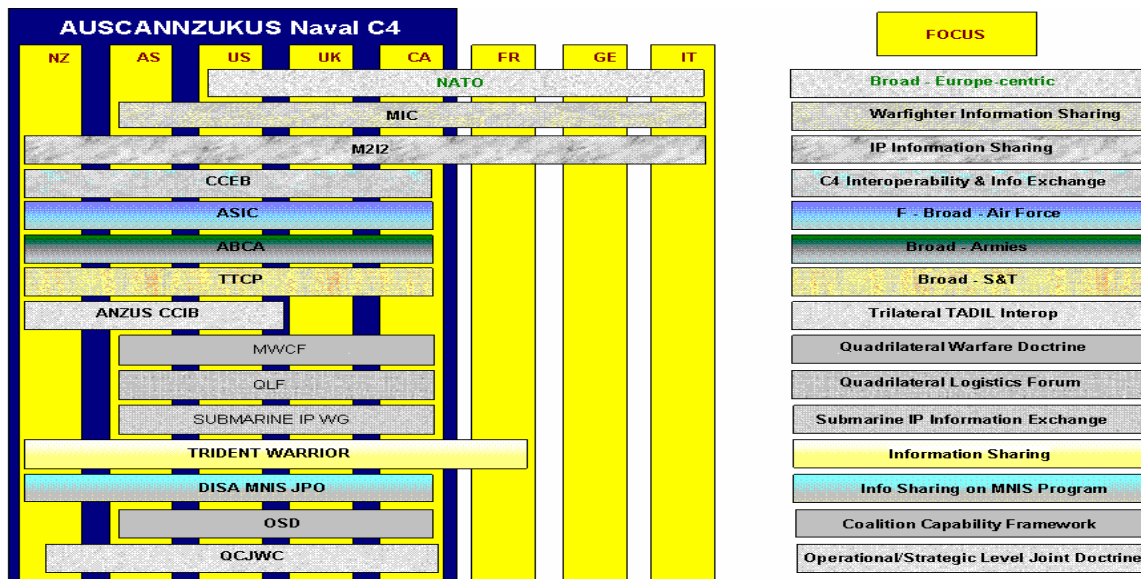


Figure 7-9  
AUSCANNZUKUS interoperability focus

**CENTRIXS In-Service Engineering Agent (ISEA)**

SPAWARSYSCEN Charleston has been designated as the ISEA and provides onsite and remote shipboard software, hardware and technical support for both systems. All requests for technical support should be directed to the ISEA. Prior to deployment, the ISEA will configure the HFIP and SNR controllers that enable Strike Group units to seamlessly form the Ad-Hoc HFIP and SNR sub-networks. With the support of AUSCANNZUKUS representatives, coalition ships are also configured prior to deploying with the

appropriate configurations required to form the Ad-Hoc HFIP and SNR sub-networks with USS ships installed with HFIP and SNR.

### **Concept of Operations**

A Concept of Operations (CONOPS) document developed by OPNAV N6, PMW-170 and AUSCANNZUKUS describes the use of the HFIP/SNR Communications systems and associated platform specific radio equipment during application of command, control, communications, computers and intelligence (C4I) operations involving ships, aircraft, submarines and shore stations. Further, this CONOPS distinguishes the use of HFIP/SNR systems in an Allied/Coalition or US Only operating environments. For more information concerning HFIP, SNR and this section, contact the following POCs.

### **Points of Contacts**

Space and Naval Warfare Systems Command (SPAWAR) PMW-170 HFIP/SNR APM Mr. Lindell Edwards at (619)524-7571, lindell.edwards@navy.mil

Chief of Naval Operations Allied Interoperability Assistant and AUSCANNZUKUS Rep LT Joe Zuliani at (703) 601-1409, joseph.zuliani@navy.mil

Space and Naval Warfare Systems Center, Charleston SC Det STL Juliens Creek DAPM-ISEA Mr. James (Jay) Smith at (757)558-6863, james.smith5@navy.mil

Space and Naval Warfare Systems Command FORCENET Allied Interoperability, Trident Warrior Coalition Lead Engineer and AUSCANNZUKUS Rep Mr. Martin Jordan at (858) 537-0109, martin.jordan@navy.mil

Space and Naval Warfare Systems Center San Diego Gov Engineer Mr. Jonathan Chan at (619) 553-7903, jonathan.chan@navy.mil

**THIS PAGE INTENTIONALLY BLANK**



## CHAPTER 8

### COLLABORATIVE TOOLS

#### 8.1 COLLABORATION AT SEA (CAS)

CAS is a set of tools that allow replication of information. CAS provides deployed naval personnel the requisite knowledge for sound decision-making. The goal of Collaboration at Sea is to support a Network Centric Operation by enhancing the Speed of Command and Improving Situational Awareness through Close Coordination and Collaboration. CAS allows a geographically dispersed/mobile organization to collaborate around the world using a web browser as the least common denominator. CAS is a tool set that allows users to share knowledge and information around the world using minimum bandwidth.

CAS has a menu system that is completely customizable by the Web site administrators. Each Web site will have designated individuals who are tasked with its maintenance. These site administrators may be on multiple locations or in one place. The distribution of this workload is at the discretion of the Knowledge Manager. The web applications allow content providers to post data using only a web browser. These applications do not require personnel be trained in Webmaster skills (HTML coding, web design, layout, etc.). Thus allowing the content provider to focus on the quality of the content (e.g. ESG, CSG, JTF, etc.), vice the mechanics of display.

Ships update their web servers through their SIPRNET connectivity to the closest NOC. Replication is done hourly but can be more frequent if the operational situation requires. Due to server size and bandwidth limitations, ships receive only the website of their assigned SG. CAS has implemented selective replication allowing low bandwidth units to replicate only the large files requested vice all documents. If a shipboard user wants to access another SG's website, they must browse off the ship to the NOC. Sametime chat servers are also located at each NOC and several CVNs, where they provide chat and whiteboard capabilities to each SG. SGs can use Microsoft Net meeting if necessary, but Sametime and Net meeting clients are not compatible, and therefore cannot talk to each other.

##### 8.1.2 IBM SAMETIME

IBM SAMETIME is a DISA Net-Centric Enterprise Services (NCES) program collaboration tool that allows Naval units to dynamically interoperate within a joint environment. IBM SAMETIME provides a variety of capabilities including instant messaging, web conferencing and persistent group chat rooms. Instant messaging and web conferencing both include point-to-point audio and video

support, while web conferencing adds shared whiteboards and desktop/application sharing. The chat rooms enable users to review activity and associated documents independent of other users. A history feature captures user messages and activity over time in a shared area so information can be revisited when needed. Due to RADIA packaging issues associated with the NMCI network, additional presence and awareness features such as a global access list, primary contacts list, local saving of chat transcripts, and creating groups and sub-groups are not accessible with the current IBM SAMETIME version 7.5.1. RADIA packaging issues will be resolved with IBM SAMETIME version 8.0 which is projected for mid to late 2008.

Availability on Navy enterprise networks. In the classified environment, IBM SAMETIME is fully available for use on the Navy Marine Corps Intranet (NMCI SIPRNET) and the OCONUS Navy Enterprise Network (ONE-NET SIPRNET) and available with limitations on the NMCI NIPRNET. Current NMCI NIPRNET firewall settings cause audio and video degradations when used with instant messaging or web-conferences, but efforts are underway to resolve firewall configuration without compromising network security. For afloat customers, IBM SAMETIME is available for use on classified and unclassified Information Technology for the Twenty-First Century (IT-21) networks. Due to bandwidth constraints, this capability will be limited to essential combat spaces such as the Combat Information Center (CIC).

Navy Telecommunications Directive (NTD) 13-07 (ALCOM 190/07) provides specific instructions (to include registration of accounts) for IBM SAMETIME use. This NTD may be viewed on the NETWARCOM Enterprise Work Space (NEWS) at: <https://www.fleetforces.navy.mil/netwarcom/readiness/spa/standardsandpolicy/n351/default.aspx>.

### **8.1.3 PERSISTENT CHAT (PCHAT)**

CHAT is a synchronous real-time system. If a user joins a CHAT session late, or drops out of an existing session, there is no record of the discussion that has taken place during the period of absence. Persistent CHAT is a tool that allows users to recall CHAT conversations within a CHAT room to review information previously passed. The room will also remain available as users come and go from the application. It is used in most cases as the primary means of collaboration for CENTRIXS.

### **8.2 TASK FORCE WEB/NAVY ENTERPRISE PORTAL**

The purpose of the Navy enterprise portal (NEP) architecture is to provide a tool for transformation of the Navy to a web-based

business and operations capability. By using the Navy NEP architecture as a tool, "as-is" architectures can be developed that will facilitate the transformation of the Navy. Many of these "as-is" systems are complex and interrelated to other systems. By using the NEP as a tool these systems migrate toward common implementations of hardware and software solutions. In addition, the architecture encompasses the resources and plans currently being developed for the network-centric infrastructures and services. The goal is to better enable Navy personnel to perform their mission by providing enterprise-wide access to knowledge bases and IT tools.

### Navy Enterprise Portal Architecture

The NEP framework is presented as a three-tiered architecture describing where the different technologies reside. The three tiers – presentation/client, application, and data/content – are described below:

1. Presentation/client – The presentation/client tier focuses on browser-based implementations and other devices such as personal digital assistants (PDAs) or cellular phones. At present, the NMCI configuration requires Microsoft's Internet Explorer (IE). IE supports the display of hypertext mark-up language (HTML), dynamic hypertext mark-up language (DHTML), and extensible mark-up language (XML), and can access data sources via hypertext transfer protocol (HTTP) and hypertext transfer protocol secure (HTTPS).

2. Application – The application tier consists of both application logic, often referred to as "components," and the server that supports these components, which is referred to as the application server. "Component Based Design" is the commercial term applied to the process of developing individual, functionally segregated application logic that can be integrated to form higher level applications. Implementing a component-based design process is the underlying strategy for providing an integrated, interoperable NEP.

Application servers provide supporting infrastructure for the components. At the application layer, enterprise-wide systems are recommended. Java 2 Enterprise Edition (J2EE) is the preferred distribution object model. J2EE is based upon open standards that promote common interfaces for object use, storage, and run-time interactions. However, minimum standards and message formats are provided that ensure interoperability with networks Navy-wide, joint, or coalition.

3. Data/content – Web content is typically derived from either static HTML files stored on the web server, or from dynamic data, as in a database. Static HTML is easy to create, but is difficult to maintain on large websites because the look and feel of the website is stored inseparably from the data. The best commercial software development practices dictate that the look and feel of the presentation should be separated from the content, allowing

them to be managed separately. Data can originate from a variety of sources including relational databases, local file stores, legacy systems, e-mail systems, groupware systems, directories, search engines, other web services, intelligent agents, and even other websites. Information sources may also be information consumers, resulting in bidirectional information flows. At the data/content layer, application logic may use a range of data source access methods; however, primary relational databases will be accessed with structured query language via Java database connectivity (JDBC) or open database connectivity.

Each of the three tiers (and the overall structure of NEP) is supported by information assurance and interoperability.

1. Information assurance is provided at each of the tiers. At the presentation/client tier, users must authenticate to their workstations and to the portal server. It is strongly desired that the user will use the DOD public key infrastructure (PKI)-issued digital certificate stored in the common access card (CAC) to authenticate to the portal server. At this tier, the web browser and the portal server communicate over HTTPS. At the application tier, the portal uses HTTPS for user interaction and provides access control, content management, centralized administration, and software application services. At the data/content tier, the portal must authenticate itself to the application to obtain information requested by the user. All transactions between the portal and the application accessing the content are audited for security purposes.

2. Interoperability is the inter/intra-tier interface between and within each of the components in the NEP architecture. Standards and technologies are used to communicate between and within the levels of the three-tier architecture. Interfaces to data, registering services, querying through a common interface, and interfaces to services are all used to communicate between and within each of the three tiers.

### **8.3 INTRA-AMPHIBIOUS READY GROUP DISTRIBUTIVE COLLABORATIVE PLANNING (IDCP)**

IDCP is a capability provided to amphibious platforms. This capability includes voice, IP data, and VTC exchanged over a wideband LOS RF path. Four key systems make up the IDCP set:

1. DWTS
2. TSS
3. ADNS
4. TAC-VTC

#### 8.4 DEFENSE COLLABORATIVE TOOL SUITE (DCTS)

The DCTS is a flexible, integrated set of applications providing interoperable, synchronous, and asynchronous collaboration capability to the DOD's agencies, combatant commands, and military services. The DCTS program identifies, fields, and sustains a dynamic set of evolving standard collaboration tools that bridge between the DOD and the intelligence community. These tools enhance simultaneous, ad hoc crisis and deliberate continuous operational action planning (vertically and horizontally) across operational theaters and other domains that provide operational units and defense organizations simultaneous access to real-time operational, tactical, and administrative information.

DCTS offers voice and video conferencing, document and application sharing, instant messaging, and whiteboard functionality to support defense planning. It enables two or more distributed operational users to simultaneously participate in the mission-planning process without the need to be collocated. With DCTS, military forces enjoy the capability to link various C4I and mission-planning systems together on a common network to share data, conduct collaborative planning, and collaboratively consult on information and data at various locations around the world. Full utilization of DCTS for video and application sharing is too bandwidth-intensive for effective shipboard use.

**THIS PAGE INTENTIONALLY BLANK**

## CHAPTER 9 VOICE COMMUNICATIONS

### 9.1 GENERAL

This chapter presents an overview of voice communication capabilities within the Navy and is intended to only serve as a ready reference guide. For amplifying information, consult current operational orders (OPORD's), OPTASK COMMS, Communication Information Bulletins (CIB's) and ACP 125 (F).

### 9.2 FREQUENCIES

Cognizant FLTCOM's control voice frequencies and promulgate them through area NCTAMS CIB's. If frequencies are not known or are of poor quality, aircraft or forces afloat may make initial contact for voice services using Advanced Digital Voice Terminal (ANDVT), SATHICOM, or full period terminations. In addition to requesting a suitable frequency, the unit will provide the precedence of the call, activity to be called, and the date and time the connection is required. The NCTAMS/NAVCOMTELSTA concerned will coordinate the call and provide a suitable working frequency.

### 9.3 CALL SIGNS

A station may be identified by several types of call signs including the unit's name, aircraft tail number or an assigned JANAP 119 or daily changing call sign. Fleet Commanders communications operating plans will prescribe the specific form of call sign to be employed based on the network used, operating conditions, type of voice report and intended recipient of the voice report.

1. The JOINT VOICE CALL SIGN BOOK contains voice call signs (words) assigned for the following:
  - a. U.S. Air Force (for further assignment)
  - b. U.S. Coast Guard ships and activities
  - c. U.S. Marine Corps activities (including lists of voice call signs for further assignment by area commands.
  - d. U.S. Naval activities and ships
  - e. U.S. Coast Guard, Marine Corps and miscellaneous aircraft assignments
  - f. Task organization
  - g. local and/or temporary assignments by U.S. Unified and Specified commands and Naval Commanders to

subordinate units and to certain foreign components when operating under operational control of U.S. forces.

- h. Convoys
- i. Amphibious assault and fire support units
- j. 10. Gunnery practice (training)
- k. 11. Search and rescue and scene of action operations
- l. 12. U.S. unified and specified commands and other activities assigned voice call signs for joint use.

2. Voice call signs may consist of one of the following types:

- a. Words
- b. Words plus letters A through Z (spoken phonetically)
- c. Words plus digits 0 through 9 (Zero, One, etc)
- d. Digit(s) plus words

3. The limited number of English words suitable for assignment as voice call signs, which are not obnoxious or ambiguous has dictated the Joint practice of assigning voice call signs at random and without consideration of actual word connotation. A voice call sign is designed for use in establishing and maintaining voice communications, and should not be considered to have any personal connotation.

4. Reassignment of voice call signs should be necessary only when it is apparent that the assigned call is ambiguous.

#### 9.4 KICK PROCEDURES

KICK procedures are used to shift to a pre-arranged secondary frequency without specifying the new frequency in the transmission. If imitative communications deception is degrading communications (or some other problem such as atmospherics on HF network) the net control station will implement KICK procedures. An example of KICK procedures is provided in Figure 9-1.

KICK Example
<p>"COLLECTIVE THIS IS ROMEO FIVE SIERRA (NECOS) KICK TWO, TIME 1532 AUTHENTICATION IS BRAVO ZULU, OUT."</p> <p>Each Number following KICK has a meaning, 2 = shift to sec. freq, 3 = shift to tert. freq, ...etc.</p>

Figure 9-1

KICK procedure example



## 9.5 RADIO VOICE LOGS

Whenever practical to do so, radio logs are to be maintained on all radio nets. Not all types of stations will be able to keep a full log. The operator in an armored fighting vehicle is not expected to maintain a log as neatly or completely as say a watchstander on a ship or headquarters who is dedicated to a single task.

Subject to the above, the radio log should contain a complete and continuous record of all transmitted and received messages, and information concerning the radio net. The log should be written legibly in the operator's own hand, and include all relevant details and timings of the following:

1. All transmitted and received informal messages and voice conversations in full or, where this is impractical, the gist of a message in sufficient detail to provide adequate reference information. Operators should attempt to log messages between other users of the radio net, but it is accepted that the logging of traffic between third parties is likely to be of second priority during busy periods.
2. The identity of formal messages written separately on a message form.
3. The opening and closing of the radio stations on the net.
4. Changes in operating frequency and interference reports.
5. Sufficient reference data to identify all other calls or procedural messages transmitted or received on the net.
6. Entries to the effect that the radio receiver is operating correctly in the receive condition. (These should be made at regular intervals during periods of net inactivity.)
7. Reports of stations with whom contact is difficult or suspect, amplified with any corrective action taken.
8. Unusual occurrences such as procedural or security violations, or suspected deception or jamming. Entries should include the reporting action taken.
9. Handover and takeover by the radio station operators. The receiving operator is to record his rank, name and signature to the effect that the transfer has been completed satisfactorily. Unless other arrangements exist, this signature is also to confirm that a complete check of any classified material has been made.

Good log keeping is an essential part of the efficient operation of a radio station, particularly at Control where the operator is

responsible for other stations on the net. Radio logs to be held in safe keeping in accordance with national / theater / command instructions.

#### **9.6 SECURE VOICE COMMUNICATIONS (FLEET ACCESS TO SECURE VOICE)**

Aboard many afloat commands, the need to interface manual shore based interconnection systems for secure voice has been overcome by the development of robust continuous-access voice and data systems such as Commercial Wideband Satellite Program (CWSP) and Defense Satellite Communications system (DSCS). DSCS and CWSP provide dynamic commercial bandwidth-on-demand for Plain Old Telephone System (POTS), Secure Telephone (STE) or STU-III, FAX, targeting imagery, and Battle Group Email. Combined with DSCS satellite bandwidth, DSCS and CWSP provides an aggregate bandwidth of 768Kbps or more to empower the warfighter with connectivity on par with ashore counterparts. This growing capability, in concert with more powerful data compression techniques, will give the warfighter the ability to access and deliver information almost instantaneously.

The Tactical Shore Gateway (TSG) has been developed to access and interconnect existing and future secure voice communications subsystems and equipment. Naval Secure Voice Subsystems incorporate major terrestrial (wireline), SATCOM (both UHF and SHF), and HF secure communications links. The SRWI is an integrator of those systems, developed primarily to alleviate limitations of existing Fleet Secure Voice Links and provide interoperability of existing and planned subsystems and equipment.

The SRWI provides the capability to connect the shore-base worldwide wireline systems with the SATCOM, Defense Satellite Communications Systems (DSCS), and alternate HF systems. The system effectively extends shore communications seaward and provides the same secure voice telephone communications to commands at sea that are currently provided to the worldwide shore establishment. The SRWI provides interconnection with or among the Secure Voice Improvement Program (SVIP) channels (STU-III/STE units), a RED telephone bus, the Advanced Narrowband Digital Voice Terminal (ANDVT) AN/USC-43(V) SATCOM radio terminals (UHF, SHF, and in the future, EHF).

The SRWI is a manned subsystem that provides operator (manual) control of the secure voice operations. Calls may be initiated from either ashore or afloat with initial contact being made with a shore operator at the appropriate NCTAMS or NCTS servicing the afloat subscribers. The shore operator can interface any two compatible subscribing channels. The operator can monitor one side of any communication in progress (except when designated private) and can also act as a net control.

## CHAPTER 10

### COMMERCIAL COMMUNICATIONS AT SEA

#### 10.1 SHIPCOM (AT&T)

ShipCom is the United States' only provider of HF SSB radiotelephone ship-to-shore service through its network of public coast stations. ShipCom also provides VHF radiotelephone, ship-to-shore and shore-to-ship radio-telex, telegrams, HF SSB email, and satellite communications.

ShipCom is the United States only 24 hour provider of HF SSB radiotelephone and VHF radiotelephone Ship to Shore voice service. ShipCom stations WLO WCL KLB and KNN are all remotely controlled from Mobile, Alabama where operators are on duty 24 hours per day 7 days per week for radiotelephone Ship to Shore and Shore to Ship calls.

#### **Email**

ShipCom provides radio email service via HF SSB radio. The ShipCom system supports SITOR, AMTOR, PACTOR and PACTOR II. No special software is needed to access the ShipCom email system. Vessels equipped with GMDSS HF SITOR may send email via the ShipCom system using the SITOR TELEX terminal. Special software now enables crew members on any vessel to setup an account with ShipCom which will allow them to access Internet email via the ship's SITOR TELEX system without any charges being incurred by the vessel. Vessels equipped with Pactor and Pactor II modes of transmission enjoy faster throughput and the full ascii character set. The ShipCom email system also offers weather, news and sports information.

ShipCom does an hourly FEC broadcast on each of the simplex channels listed under frequencies. This broadcast may be used for tuning purposes and to determine which ShipCom frequency provides the best signal. To access the ShipCom email system, simply tune your radio to the appropriate frequency as found under frequencies on this web site. For SITOR/AMTOR modes place an ARQ call to 1090 (XVSV). For Pactor modes, Pactor call WLO-1. Vessels must be registered with ShipCom in order to send and receive email and weather information. Operators are available 24 hours daily for assistance if required. Type OPR to access the ShipCom operator.

#### **Fax**

Vessels using ShipCom's SITOR or Pactor systems may send text messages to any fax machine world wide. Messages are composed on the ship's SITOR terminal and are sent to any fax machine using the send fax command. While it is possible to send a fax message from Shore to Ship on suitably equipped vessels, ShipCom does not recommend this practice as delivery is usually difficult and the

sender is charged for failed delivery attempts.

### **Satellite**

ShipCom can send messages to any satellite terminal in the world. Messages may be billed to Visa, Master Card, Discover, American Express or to your home or business telephone. Messages to satellite terminals should be addressed to [wloradio@wloradio.com](mailto:wloradio@wloradio.com) and must include the Vessel name, radio callsign, MMSI and the satellite number if known.

### **Telegrams**

ShipCom can send radio - telegrams to most any ship in the world. Telegrams may be billed to Visa, Master Card, Discover, American Express or to your home or business telephone. The charge for sending a radio-telegram to a ship is \$25.00 for the first 50 words.

### **VHF**

ShipCom provides VHF radiotelephone service to a typical distance of 50 miles off shore from the above locations. To access the ShipCom operator select the appropriate channel and hold your transmit key for 5 seconds. The charge for VHF radiotelephone service is .99/minute with a 3 minute minimum. Calls may be placed collect to anywhere in the United States.

### **Telex**

Vessels equipped with SITOR can send directly connected Telex messages to any telex terminal in the world. Vessels can also send store and forward Telex messages. Store and forward Telex messages are less expensive and usually arrive within minutes of transmission. Telex messages may be sent from shore to ship by sending the telex to 6827072 or 505444. The message should include the Ship Name and Radio Callsign and MMSI number. Telex messages may also be sent by emailing to [wloradio@wloradio.com](mailto:wloradio@wloradio.com). The email containing the Telex message should also contain the Ship Name, Radio Callsign and MMSI number. ShipCom will deliver Telex messages via radio or satellite to the vessel. Parties sending Telex messages sent with PC (paid confirmation) will receive notification of successful delivery of the message to the Ship.

### **Weather**

The ShipCom operators can provide vessels with weather information and are always available should an emergency ever arise while you are at sea. Using ShipCom is simple. Simply tune your radio to the appropriate channel as listed on our frequencies page. Call one of the ShipCom stations by depressing your microphone and saying WLO WLO WLO this is the M/V My Ship

calling on channel 824. The operator will ask you for your position and will optimize the radio circuit before placing your call. For Shore to Ship calls, the calling party should give the operator the name of the vessel and radio callsign. ShipCom will broadcast a list of vessels that we are holding calls for at the top of each hour following the weather broadcast.

ShipCom transmits hourly weather and traffic list on selected ITU HF SSB voice channels. For a schedule of the weather products and broadcast times see the frequencies page. Virtually any weather product is available via ShipCom's HF SITOR / Pactor system on demand. All ShipCom weather products are automatically updated from the National Weather Service. Vessels sending AMVER and OBS messages are entitled to receive free weather products via SITOR or Pactor. For more information on the AMVER/OBS programs ask your ShipCom operator.

**THIS PAGE INTENTIONALLY BLANK**

## CHAPTER 11

**INFORMATION ASSURANCE/COMPUTER NETWORK DEFENSE****11.1 INFORMATION ASSURANCE**

**11.1.1 IA Reporting:** When a user or system administrator suspects a computer security incident, he/she must contact the command Information Assurance Manager (IAM). The IAM has primary responsibility for informing the Chain of Command and is also responsible for collecting as much information as possible about the event. The local IAM does not have the authority to declare an event an incident. Only the **Navy Cyber Defense Operations Command (NCDOC) can declare an incident.**

**11.1.2 Malicious Code and Viruses:**

The threat of attack from a computer virus or other malicious code, both deliberate and inadvertent, is significant. Successful virus prevention incorporates technical, policy and procedural elements.

All DoN Information Systems and networks shall use anti-virus software to intercept viruses before they can establish themselves. Commands shall develop and implement local policy and procedures to support effective employment of anti-virus software and should address:

1. Program and Macro Viruses
2. Java and Active-X Scripts
3. Diskettes
4. Notebook and Privately Owned/Home Computers
5. E-mail Attachments
6. Downloaded and Remotely Transferred Files

As the nature of the threat from virus software constantly changes, sites shall ensure that antivirus software profiles are updated on a routine and frequent basis. DoD licensed anti-virus software is available free to all DoN activities and may be downloaded from the DoN INFOSEC Web Site:

- o NIPRNET <https://infosec.navy.mil>
- o SIPRNET <http://infosec.navy.smil.mil>

This software is also authorized for, and should be installed on, personal computers privately owned by DoD personnel and used for official business. PEO C4I and Space (PMW-160) can provide

assistance in designing optimal technical solutions to combat virus software.

### **11.1.3 ANTI-VIRUS SOFTWARE:**

Updating anti-virus software so that it contains the latest virus definitions will decrease the likelihood that any command supported equipment will be affected by a new type of virus.

The following procedures shall be adhered to by all users in the utilization of anti-virus software:

1. Ensure that the anti-virus program is scanning all incoming E-mail attachments and all files or programs that come from someone else's computer. Whenever someone puts a file or a program on their computer, there is always some risk that a virus may infect that file or program and remain undetected.
2. Ensure that the approved anti-virus program is regularly updated as prescribed by SPAWAR/PEO C4I. This will minimize the threat of new or improved viruses unleashed through the Internet that could potentially infect your command.
3. Finally, ensure that spot checks are executed on a regular basis to ensure that the command anti-virus software provides regular updates to IDS signatures.

### **11.1.4 GUARDING YOUR PC AGAINST VIRUSES:**

A personal computer (PC) virus is a program that can reproduce itself and spread from PC to PC, usually without you knowing it. Some viruses deliberately destroy documents or data files, others can put messages on your screen or otherwise create a nuisance and interrupt your work. They may be present in files, particularly software (executable files) and Word files (documents and templates). They may also be present in the hidden system areas of disks (the partition sector of hard disks and the boot sector of floppy and hard disks). It is possible that a virus may be present on disks that apparently contain no files.

The most tenacious viruses are passed through Word and Excel macros. NCDOD handles virus reporting in the Navy and USMC per CNO Message 111754Z OCT 95. Additionally, Symantec publishes a table of regional outbreaks on <http://securityresponse.symantec.com>.

### **11.1.5 KEEPING YOUR PC VIRUS-FREE**

All PC users should take precautions to detect viruses and prevent their spread. A quick anti-virus strategy for all PCs might be:



1. Prevention: adopt good, virus-awareness habits of PC use. Taking simple precautions can prevent many hours of tedious work required to disinfect a PC should a virus occur.
2. Detection: viruses can normally be detected only by the use of special virus-detection software which can also be downloaded from the INFOSEC website.
3. Cure: promptly eliminating viruses if/when found. The NCDOC support staff can assist and provide alternative methods for virus elimination. The Navy's INFOSEC Help Desk / Service Center (1.800.304.4636) can also assist you with the Anti-viral Software and virus problems.

Some helpful hints in maintaining your PC virus free:

1. Beware of an e-mail message with a binary file attachment. You can catch a virus from a binary file attachment to an e-mail message, like the MIME or Uuencoded files that are normally sent over the Internet. If you receive a binary file, scan it with a virus scanner before opening it.
2. Install a memory-resident virus checker to detect suspicious program activity. Norton and McAfee Anti-Virus are good choices. Also, regularly scan your hard disk for viruses. Home PCs are often infected by your children or yourself passing diskettes around, by disks from the office, or by computer repair shop diagnostic disks. This is one of the largest points of entry for DoD infections.
3. Scan anything you download off the Internet or online services. Some software packages do this for you. Ideally, you should download programs to a floppy and then scan them before copying them to your hard disk.
4. Use several types of virus scanners. A virus that slips past one product might be picked up by another.
5. Disable Java/JavaScript in your browser unless you're visiting a TRUSTED Site. Java is a very powerful tool and works by downloading executable files to your PC. Security is built in, but Java may contain holes for virus makers to exploit. Caution should be exercised when you notice JAVA running.
6. Scan all portable media brought into your Command.

## 11.2 COMPUTER NETWORK DEFENSE (CND)

NCDOC is the Navy's Computer Network Defense Service Provider (CNDSP) and is governed under policy as outlined in DoD O-8530.1M,

DoDI O-8530.2, CJCSM 6510.01 and NETWARCOM Instruction 5450.4. NCDOC responsibilities involve, but are not limited to, the following:

1. 24/7 CND Service Subscriber Support: NCDOC maintains a 24/7 watch that monitors the defensive readiness of Navy NIPRNET/SIPRNET networks and aggressively fights the net through detection and analysis of adversarial operations. NCDOC personnel pro-actively detect, deter, respond, and remediate intruder threats within Navy networks, including malicious activity (either internal or external in origin) and malicious logic (computer viruses, worms, etc.). NCDOC will provide tailored assistance and recovery recommendations and/or directives to Navy commands involved in cyber incidents.
2. Navy Enterprise Sensor Grid: NCDOC monitors and oversees the operation of the Navy Enterprise Sensor Grid and all Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) capabilities in place on Navy NMCI, BUMED, Excepted (legacy) and ONENET networks. The recent conversion of IPS sensors at Network Operation Security Centers (NOSCs) and Fleet Network Operations Centers (FLTNOCs) provide a proactive defense mechanism designed to detect malicious activity across all Navy enclaves, including IT-21. The Navy Enterprise Sensor Grid provides an optimized, robust, joint interoperable computer network defense capability enhancing the Navy's defense in depth strategy.
3. Vulnerability Assessment (VA) Support: Vulnerability assessments are a critical contributor to CND operational readiness and essential as a means of measuring the posture of DoD information systems and computer networks. NCDOC conducts directed network vulnerability scanning to check for compliancy with IAVM, UTN-P Policy and STIGs.
4. Notifications: NCDOC will notify CND service Subscribers of activity that may adversely affect Navy networks. These notifications will be in the form of NCDOC advisories and alerts. The advisories/alerts will be disseminated via record message traffic (DMS) and will include maintenance actions, power outages affecting sensors or other CND capabilities, virus outbreaks, network threats and vulnerability assessments. NCDOC will also notify CND Service Subscribers upon completion of an incident investigation.
5. Information Assurance Vulnerability Management (IAVM): The IAVM Process is one of the core components of both the Navy's and the Joint Forces Information Assurance Program. IAVM is the process by which emerging vulnerabilities are identified and corrected throughout the DoD. The Assistant Secretary of Defense has the overall responsibility for the implementation of the IAVM program policy and procedures

across all C/S/As and field activity. USSTRATCOM is responsible for maintaining overall responsibility for IAVM program execution. JTF-GNO is responsible for monitoring relevant sources of information to discover security conditions that may require IAVM vulnerability notification, assessing risk associated with software vulnerabilities and developing IAVM vulnerability notifications. JTF-GNO reports directly to USSTRATCOM and is responsible for integrating, coordinating, and executing computer network operations across the joint services.

Upon detection or reporting of a new vulnerability, JTF-GNO will validate the presence and impact of the vulnerability. In the event JTF-GNO determines the vulnerability poses an immediate risk to DoD systems, an Information Assurance Vulnerability Alert (IAVA) will be issued. At a minimum, the IAVA will contain a summary of the vulnerability, its probable impacts, and any countermeasures or actions JTF-GNO may direct.

Within the Navy, NCDOC is responsible for all CND operations. When an IAVA message is received, NCDOC is required to immediately notify all affected Navy units and coordinate compliance activities across the entire Navy. NCDOC is required to take corrective action within 30 days and report back to JTF-GNO with the Navy's compliance statistics. When in receipt of an IAVA, Navy units will take the following actions:

1. Navy units must confirm acknowledgement of IAVAs by identifying and submitting report of affected assets in the Online Compliance Reporting System (OCRS) no later than 4 days (additional days if they fall on a weekend) after release. Units must comply within the compliance date, generally 30 days. If they are unable to meet compliance deadline, a mitigation plan must be submitted and approved for non-compliant assets.
2. Navy units must confirm acknowledgement of IAVBs by identifying and submitting report of affected assets in the OCRS no later than 4 days (additional days if they fall on a weekend) after release. Units must comply within the compliance date, generally within 45 days or less. If they are unable to meet compliance deadline, a mitigation plan must be submitted and approved for non-compliant assets.
3. Navy units will acknowledge receipt of CTOs based on criticality (usually 4 days, but may be adjusted). Units will comply with CTOs based on criticality as defined by NCDOC/NETWARCOM.
4. NCDOC will notify the DAA in situations where IAVA compliance cannot be achieved in a timely fashion, when applicable. The DAA may recommend disconnection from the GIG. In certain cases, the DAA may approve commands or Programs of Record (POR) to operate in a high risk status for a short

period of time. This typically applies to Programs of Record (POR) that require formal configuration control and testing prior to deploying any new patches. These waivers are not permanent and the POR is required to address the IAVA. In some situations where IAVA compliance could adversely impact the operational capability of the Fleet or an individual ship, the ship's CO has the authority for non-POR systems to issue a temporary waiver until such time as the immediate operational situation is resolved. NETWARCOM has the authority to not publish IAVM messages if they determine there will be a major impact to the fleet, etc.

5. Threat Analysis and Network Forensics: TANF provides predictive analysis on emerging threats to the Global Information Grid (GIG) and post incident forensic analysis on successful and unsuccessful cyber attacks. TANF provides several products and reports containing actionable indications on warning information to allow warfighters to better fight the net. The following reports are available at the NCDOC SIPRNET website [www.ncdoc.navy.smil.mil](http://www.ncdoc.navy.smil.mil). Additionally, NCDOC provides unclassified versions of reports via record messages:

- a. Cyber Alert (CA): Actionable report of immediate threat activity targeting the Global Information Grid (GIG). These reports normally require immediate attention and are intended to provide proactive actions to network defenders. An unclassified CA summary is also sent via record message to maximize dissemination.
- b. Network Analyst Report (NAR): An event or activity driven report containing multi-sourced fused analysis that combines current or emerging trends with specific threat indicators to provide enhanced situational awareness.
- c. Cyber Technical Report (CTR): Report that provides detailed findings from forensics investigations of confirmed intrusions based on logs, raw packet data and media image analysis. Report provides network defenders and analysts detailed technical information to assist in hardening the defense of the DoD GIG.
- d. Cyber Technical Report-Malware Analysis (CTR-MA): Report that details reverse engineering findings of malware discovered on the Navy portion of the GIG.
- e. Incident Trends Report (ITR): Monthly/yearly historical report trending Navy CIRT Database (NCD) incidents and events reported to NCDOC. Report provides trending data by COCOM, enclave, mission area, and other incident related statistical metrics.

CJCSM 6510.01 is fairly broad on what constitutes a reportable event. However, an IAM does have some degree of latitude in reporting, and should conduct sufficient preliminary investigation to determine if an event can and should be resolved at the local level prior to submitting an incident report.

All events of interest from a security perspective should be tracked and, in cases where a violation of policy that can be resolved at the local level, the CO should be informed. Prior to reporting a suspected incident to NCDOC, the XO and/or CO should be notified. Note that in cases where an event clearly meets the reporting criteria of CJCSM 6510.01 it must be reported, even in cases where the CO would like to resolve the situation locally.

In cases where an incident report will be submitted to NCDOC, the IAM will be the local point of contact for resolution. In the CSG/ESG this will also include coordination among the other IAMs in the strike group. In situations where the suspected incident occurs on board an aircraft carrier, the IAM must coordinate with his/her counterpart in the air wing as well.

Upon receipt of an incident report, NCDOC will evaluate the information received, request and/or direct follow up investigation, and make a determination of whether or not a computer security incident has taken place. For each incident report received, NCDOC will author a follow-up report and alert the appropriate Navy and/or government entities. The detecting IAM will coordinate and implement the NCDOC directed follow-up investigation and will take recovery actions as directed. In extremely severe cases it is possible NCDOC will send an Incident Response Team to assist in resolving the incident.

There are several ways in which to report an incident:

1. NIPRNET Email ([NCDOC@NCDOC.navy.mil](mailto:NCDOC@NCDOC.navy.mil))
2. SIPRNET Email ([NCDOC@NCDOC.navy.smil.mil](mailto:NCDOC@NCDOC.navy.smil.mil))
3. Phone (Non-Secure): (888) NAV-CDOC (628-2362)
4. Fax (Non-Secure): (757) 417-4031
5. DMS Message: NAVYCYBERDEFOPSCOM NORFOLK VA
6. NCDOC Homepage (<http://www.NCDOC.navy.mil>)

CND of the Carrier Strike Group (CSG) and the Expeditionary Strike Group (ESG) is based on the concept of defense of depth, whereby a global array of organizations and technology supporting standard policies and doctrine protect Navy C4I networks from

attack in order to ensure the availability and integrity of critical systems and data. The DoD has identified four specific layers for defense in depth:

1. Host or end user systems.
2. Enclaves and the enclave boundary, in this case a shipboard LAN.
3. Networks that link the enclaves, typically WANs.
4. Supporting infrastructures.

CND for the CSG or ESG is primarily focused on the first three layers.

1. CSG/ESG CND begins at the FLTNOC. There, all IP traffic addressed to the SG goes through a sophisticated array of screening routers, firewalls, network intrusion detection sensors, and virus scanning software before being routed to the SG.
2. The WAN links between the NOC and an individual SG ship consist of satellite communication links, which vary depending on ship class and installed systems. These links are encrypted at the appropriate classification level by standard cryptographic devices. For wideband SATCOM systems such as SHF, additional bulk encryption of the entire communications channel is performed to provide transmission security (TRANSEC).
3. Shipboard, CND is provided by routers, firewalls, intrusion detection devices, virus protection software, and network monitoring tools. Exact configurations vary greatly, with CVNs and other ship classes configured with large LANs having the most comprehensive and sophisticated capabilities. The Navy is moving as much as possible toward embedded security features that are built in to both software applications and hardware in an effort to minimize network complexity and to automate CND functions.

### **11.3 INCIDENT HANDLING REPORTS**

Comprehensive reporting and responding to reportable events and incidents is vital to ensuring commanders' successful accomplishment of their operational missions and continued operation of DoD systems and networks.

Due to increased Joint and Combined operations, increased reliance on IT, increased threat to IT, and increased network centric operations requiring networks to be more resilient, the

need for standardized incident handling practices across the DoD is imperative.

Federal guidance mandates establishment of an incident response capability. The Federal Information Security Management Act (FISMA) of 2002 requires federal agencies to have in place incident detection and reporting mechanisms. Appendix III to Office of Management and Budget (OMB) Circular No. A-130 "Security of Federal Automated Information Resources" directs agencies to establish formal incident response mechanisms. DODI O-8530.01 identifies five phases of CND:

1. Protect
2. Monitor
3. Detect
4. Analyze
5. Respond

#### **11.4 BASIC INCIDENT HANDLING GUIDELINES**

If an incident is suspected to have occurred, follow these guidelines:

1. A reportable event or incident should be reported IAW CJCSM 6510.01. Events (including reportable events) and incidents should be detected, analyzed, and corrected at the level that is deemed most effective by the governing combatant command, Service, and/or agency (C/S/A) and field activity.
2. Incidents or sets of events (reportable events that may result in an incident) should be reported early. Once verified as an incident, reports and updates should be provided often and with enough granularities for all DOD analysts to determine corrective actions related to monitoring, detecting, analyzing, and responding to protect their DOD assets.
3. Incidents that may be classified in multiple categories are reported at the most severe category; e.g., a Category 1 root level intrusion incident that is caused by a less critical Category 5 Non-Compliance Activity event is reported as a Category 1 incident.
4. Deconfliction and coordination is done horizontally and vertically through law enforcement/counterintelligence (LE/CI), intelligence, technical, and management/oversight channels for assistance and situational awareness.
5. Commanders are ultimately responsible and accountable for their networks.

For more detailed information on incident reporting methodology and forms, refer to CJCSM 6510.01. Below is an example of a computer intrusion report:

FM COMMAND NAME//  
TO NAVCYBERDEFOPSCOM NORFOLK VA//  
INFO COMSTRKFORTRAPAC//  
NAVIOCOM NORFOLK VA//  
NAVIOCOM SAN DIEGO CA//  
(APPROPRIATE CHAIN OF COMMAND)//  
//CLASSIFICATION// SECRET FOR SIPRNET OR UNCLAS//FOUO FOR NIPRNET,  
REFER TO CJCSM 6510.01 CH3, PAGE 44 SECTION F FOR MORE  
INFORMATION)  
SUBJ: POSSIBLE COMPUTER INTRUSION INCIDENT//  
MSGID/GENADMIN//  
REF/A/DOC/CJCSM/8MAR2006//  
REF/B/MSG/COMNAVNETWARCOM NORFOLK VA/151503ZMAY2006//  
REF/C/DOC/OPNAV/03MAR1998//  
NARR//REF A IS CJCSM 6510.01, CHANGE 3, DEFENSE-IN-DEPTH:  
INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND)  
- APPENDIX B, INCIDENT HANDLING PROGRAM. REF B IS NAVY  
TELECOMMUNICATIONS DIRECTIVE (NTD) 04-06, COMPUTER INCIDENT  
HANDLING PROGRAM. REF C IS OPNAVINST 2201.2 NAVY AND MARINE CORPS  
COMPUTER INCIDENT RESPONSE.  
RMKS/1. CERT/CIRT INCIDENT NUMBER:  
2. PRIMARY INCIDENT CATEGORY:  
3. SECONDARY INCIDENT CATEGORY:  
4. ATTACK VECTOR:  
5. WEAKNESS:  
6. LAST UPDATE:  
7. INCIDENT START DATE:  
8. INCIDENT END DATE:  
9. STATUS:  
10. SYSTEM CLASSIFICATION:  
11. DETECTING UNIT OR ORGANIZATION:  
12. ACTION TAKEN:  
13. ORGANIZATION TRACKING:  
14. CERT DATE REPORTED:  
15. OPERATIONAL IMPACT:  
16. MAJOR COMMAND:  
17. SYSTEM IMPACT:  
18. SYSTEMS AFFECTED:  
19. STAFF HOURS LOST:  
20. EXERCISE NAME:  
21. EVENT DESCRIPTION:  
22. SOURCE IP AND PORT:  
23. INTRUDER(S) (IF KNOWN):  
24. ORIGIN (COUNTRY):  
25. TARGET IP(S) AND PORT:  
26. TECHNICAL DETAILS:  
27. PHYSICAL LOCATION (BASE, CAMP, PORT OR STATION):  
28. TECHNIQUE, TOOL, OR EXPLOIT USED:  
29. OS AND VERSION OF OS:  
30. USE OF TARGET (E.G. WEB SERVER, FILE SERVER, HOST):  
31. DOD NETWORK:  
32. COMMENTS:  
33. SYNOPSIS:



34. OPREP 3 REPORTING:  
 35. CONTACT INFORMATION:  
 NAME:  
 ORGANIZATION:  
 TELEPHONE:  
 FAX:  
 E-MAIL:

### 11.5 INFOCON

The INFOCON strategy has shifted from a threat-based, reactive system to a readiness-based and proactive approach. This represents a significant change in how commanders at all levels ensure the security and operational readiness of their information networks. CJTF-GNO will recommend changes in DoD INFOCON levels to CDRUSSTRATCOM who will, based upon necessity, direct a DoD level INFOCON change. NCDOC will disseminate global INFOCON level changes to Navy components. Combatant Commanders (COCOM) retain the authority to set regional INFOCON levels, however, regional and/or theater INFOCON levels must remain at least as stringent as the DoD level. Regional COCOMS who independently raise INFOCON levels are required to notify USSTRATCOM as time allows. NCDOC will coordinate Navy INFOCON implementation with COCOMS and Service components in advance. The INFOCON mirrors the alert system of the Chairman of the Joint Chiefs of Staff, Defense Conditions (CJCS Manual 3402.1B, Alert System of the Chairman of the Joint Chiefs of Staff) and are a uniform system of 5 progressive readiness conditions. INFOCON 5, INFOCON 4, INFOCON 3, INFOCON 2, and INFOCON 1. INFOCON 5 is normal readiness and INFOCON 1 is maximum readiness. Each level represents an increasing level of network readiness based on current operations, threats, and vulnerabilities. INFOCON specific tasks are augmented by tailored readiness options (TROS), which are applied in order to respond to specific intrusion characteristics or activities as directed by CDRUSSTRATCOM or COCOMS.

The INFOCON system relies heavily on the capabilities of system administrators to manage their networks and data systems, ensuring a heightened level of readiness for day-to-day and crisis operations. INFOCON attainment is paramount to mitigating enemy capabilities and deterring intent of computer exploitation and attacks. Specific tasks are reference in Appendix 12 to Annex C (Operations) to JTF-GNO OPORD 05-01 (Global Network Operations). The 5 progressive INFOCON levels are defined below:

INFOCON 5 - Characterized by routing NETOPS normal readiness of information systems and networks that can be sustained indefinitely. Information networks are fully operational in a known baseline condition with standard information assurance policies in place and enforced. Baseline is defined as a process allowing system administrators, either by software or manually, a means to measurable restore confidence in their information

systems. By comparing a known good baseline of each network asset to its current state, an administrator can potentially detect the presence of intruder activity. The first step in establishing a known valid baseline is accomplished when a system is first brought on line or has been rebuilt. This is a snapshot of the network in its most "pristine" state and establishes the "norm" to which all future comparisons are made. At this point, a restoration image of the operating system, critical applications and firmware should be created. The second step, referred to as validation, is the portion of the baselining procedure in which a snapshot of a current system is compared to the known valid "pristine" baseline and the changes between the two are identified and accounted for. During INFOCON 5, system and network administrators will create and maintain a snapshot baseline of critical and non-critical systems, servers, workstations (i.e., BDC, PDC, routers, etc) in a known good configuration and develop processes to update that baseline for authorized changes. Validations of the known baseline occur every 180 days.

INFOCON 4 - Increases NETOPS readiness either in preparation for operations or exercises or in response to network events, with a limited impact to the end user. System and network administrators will establish an operational rhythm to validate the known good image of an information network against the current state and identify unauthorized changes. Additionally, user profiles and accounts are reviewed and checks conducted for dormant accounts. By increasing the frequency of this validation process, the state of an information network is confirmed as unaltered (i.e., good) or determined to be compromised. Impact to end-users is negligible. This INFOCON level should be able to be maintained for a prolonged period of time as the situation dictates.

INFOCON 3 - Further increases NETOPS readiness by increasing the frequency of validation of the information network and its corresponding configuration. Impact to end-users is minor. This INFOCON level should be able to be maintained for a moderate period of time as the situation dictates.

INFOCON 2 - Is a readiness condition requiring a further increase in frequency of validation of the information network and its corresponding configuration. The impact on system administrators will increase in comparison to INFOCON 3 and will require an increase in preplanning, personnel training, and the exercising and pre-positioning of system rebuilding utilities. Use of hot spare equipment can substantially reduce downtime by allowing rebuilding in parallel. Impact to end-users could be significant for short periods. This impact can be partially mitigated through thorough training and proper sequencing of INFOCON actions. This INFOCON level should be able to be maintained for a moderate period of time as the situation dictates but it is understood it will impose significant resource challenges.

INFOCON 1 - Is the highest readiness condition and addresses intrusion techniques that cannot be identified or defeated at lower readiness levels (e.g. Kernel Root Kit). It should be

implemented only in those limited cases where INFCON 2 measures repeatedly indicate anomalous activities that cannot be explained except by the presences of these intrusion techniques. Once a baseline comparison no longer indicates anomalous activities, INFOCON 1 should be terminated. The impact on system administrators will be significant and will require an increase in preplanning, personnel training and the exercising and pre-positioning of system rebuilding utilities. Use of hot spare equipment can substantially reduce downtime by allowing rebuilding in parallel. Impact to end-users could be significant for short periods. This impact can be partially mitigated through thorough training and proper sequencing of INFOCON actions. This INFOCON level should be able to be maintained for a brief period of time as the situation dictates. NCDOC will direct Global INFOCON level changes to navy assets. In addition to the Global INFOCON level set by USSTRATCOM, COCOMS may, based on their own established evaluation criteria, raise the theater INFOCON level higher than the established DoD Global INFOCON level. COCOMS are required to notify USSTRATCOM of theater directed INFOCON changes to determine and mitigate operational impact to the GIG. NCDOC will coordinate Navy INFOCON implementation with COCOMS and service components.

#### **11.6 RED TEAM SURVEYS**

The Navy Information Operations Command Norfolk (NIOC-N) Red Team was initially formed to support the Secretary of the Navy's (SECNAV) memorandum of 24 October 1996, as a process by which to gauge the information assurance operational readiness of United States Naval Forces.

The Red Team's role in the Information Assurance process logically follows a policy review and vulnerability assessment. The Red Team may or may not be a part of the actual assessment process. Following the policy review and assessment, and a network vulnerability assessment, a penetration test can be requested by the requesting command. The Penetration test is normally conducted in two phases. Phase 1 involves the collection of unclassified information through open sources. During this phase, the Red Team will attempt to characterize the target and its systems, identify potential vulnerabilities, and concurrently analyze information gathered to plan activities to be considered for execution during the next phase. Phase 2 is the active network attack/exploit phase and requires 24/7 White Cell to ensure the scope of the exercises is maintained, and that all exercise activity ceases immediately in the case of "real world" activities. Generally, the Red Team emulates an opposition force and collects information on the target, processes the information to plan an IO attack, then carries out the attack. The goal is to improve the readiness of U.S. Forces through discovery and demonstration of information vulnerabilities and illustration of achievable adversary operational impact.

The Red Team process and application can be found at the following website: <https://www.ncdoc.navy.mil>

### 11.7 COMPUTER TASKING ORDERS (CTO)

CTOs address vulnerabilities extremely critical to the overall security of the Global Information Grid (GIG). They supersede or change current DoN Network policy and provide implementation direction for new Information Assurance (IA) initiatives. Acknowledgement is generally based on the criticality (usually 4 days, but may be adjusted). Timeline for compliance may be very short or may take years depending on what action is required in the milestones. This is also based on criticality.

JTF GNO sends vulnerability notification to Component Commands/Services and Agencies. The CTO post technical write up and/or executive summary will be posted to websites.

NCDOC will review the technical write up and provide comments/recommendations to NETWARCOM. NETWARCOM sends CTO to all Navy components and then NCDOC will post to OCRS and track compliance.

When an initiative is issued, Program Managers are responsible for testing, developing, and issuing patches to units where their Program of Record is installed.

### 11.8 PUBLIC KEY INFRASTRUCTURE (PKI)

Many programs supporting the DoD mission require security services, such as authentication, confidentiality, non-repudiation, and access control. To help address these security problems, the DoD developed PKI. The DoD PKI provides products and services that enhance the security of networked information systems and facilitate digital signatures.

Applications must be enabled to take advantage of the services a PKI offers. Without enabled applications, the infrastructure holds little value. It is essential that applications become enabled and utilize the infrastructure. However, enabling is a complicated task. Applications must be tested to ensure they are enabled correctly, and are interoperable with the DoD PKI.

The DoD PKI PMO established the Joint Interoperability Test Command (JTIC) DoD PKE (Public Key Enabled) Certification Lab as an independent facility to perform interoperability testing on PKE applications. It is DoD policy that enabled applications be tested to ensure interoperability and compatibility with the DoD PKI.

**APPENDIX A**  
**LIST OF ACRONYMS**

One of the side effects of modern communications is the proliferation of acronyms, abbreviations and code words that have come into use. This appendix is a list of common Command, Control Communications, Computers, and Intelligence (C4I) acronyms. This appendix is by no means all-inclusive. It is entered as an aid to persons new to Naval Communications and C4I systems to enable them to more easily grasp this increasingly complex field.

-- A --

AADC	Anti Air Defense Coordinator
AADS	Amphibious Assault Direction System
AAN	Advanced Alteration Number
AAP	Amphibious Assault Planner
AARC	Asymmetric ADW Resynchronization Controller
AATC	Amphibious Assault Traffic Control
AAW	Anti-Aircraft Warfare
AAWC	Anti-Aircraft Warfare Commander
ABM	Agile Beam Management
ACC	Area Control Center
ACU	Antenna Control Unit
ACAT	Acquisition Category
ACCES	Advanced Cryptologic Carry-on Exploitation System
ACL	Access Control List
ACLS	Automatic Carrier Landing System
ACTD	Advanced Concept Technology Demonstrations
ACTS	Aegis Combat Training System
ACU	Antenna Control Unit
ACDS	Advanced Combat Direction System
ACINT	Acoustic Intelligence
ACLS	Automatic Carrier Landing System
ACMS	Automated COMSEC Material System
ACMS	Automated Communications Management System
ACO	Airspace Control Order
ACT	Activation Availability
ACTD	Advanced Concept Technology Demonstration
ADA	Air Defense Artillery
ADE	Above Deck Equipment
ADMS	Advanced Digital Multiplexer System
ADNS	Automated Digital Network System
ADP	Automated Data Processing
ADS	Air Deconfliction System
ADS	Advanced Deployable System
ADS	Aegis Display System
ADSI	Air Defense Systems Integrator
ADTU	ANDVT Data Transfer Unit
ADT	Automatic Detection and Tracking
AdvHDR	Advanced High Data Rate Antenna
ADW	Advanced Digital Waveform
AEHF	Advanced EHF
AEGIS	Airborne Electronic Grid and Information

	System
AEHF	Advanced EHF
AEL	Allowance Equipage List
AER	Alteration Equivalent to a Repair
AFATDS	Advanced Field Artillery Tactical Data System
AFB	Air Force Base
AFRTS	Armed Forces Radio Television Service
AGF	Command Ship
AIC	Air Intercept Control
AIEWS	Advanced Integrated Electronic Warfare System
AIG	Address Indicator Group
AIM	Advanced INFOSEC Module
AIMD	Aircraft Intermediate Maintenance Departments
AIP	Assured IP (Internet Protocol)
AIPS	Alteration Installation Planning System
AIS	Automatic Identification System
AIS	Automated Information System
AIT	Alteration Installation Team
AJ	Anti-Jam
AKDC	Automatic Key Distribution Center
ALCND	Computer Network Defense Alert
ALE	Automated Link Establishment
ALIS	Aegis LAN Interconnection System
AMHS	Automated Message Handling System
AM	Amplitude Modulation
AMP	Advanced Message Protocol
AMPS	Afloat Master Planning System
ANCC	Automated Network Control Center
ANCC/ATC	Automated Network Control Center/ Automated Technical Center
ANDVT	Advanced Narrowband Digital Voice Terminal
ANSI	American National Standards Institute
AOA	Analysis of Alternatives
AOC	Air Operations Center
AODA	Air/Ocean Data Assimilation
AOP	Air/Ocean Prediction
AOR	Area of Responsibility
AOR	Area of Operational Readiness
AOR	Atlantic Ocean Region (W-West; E-East)
AOR-E	Atlantic Ocean Region East
AOR-W	Atlantic Ocean Region West
APG	Antenna Pedestal Group
API	Application Programming Interface
APL	Allowance Parts List
APM	Assistant Program Manager
APS	Afloat Planning System
APTS	Afloat Personal Telecommunications Service
APTS	Afloat Personal Telecommunications System
AR	Alteration Request
ARG	Amphibious Ready Group
ARGSIT	Amphibious Ready Group System Integration Testing
ARS-ST	Airborne Receiving System-Surface Terminal

ARPA	Automated Radar Plotting Aid
ASCII	American Standard Code for Information Interchange
ASD	Assistant Secretary of Defense
ASD	Asynchronous Data
ASN	Assistant Secretary of the Navy
ASCIET	Air Services Combat Identification Evaluation Team
ASCII	American Standard Code for Information Interchange
ASIU	Auxiliary Sensor Interface Unit
ASOS	Automated Surface Observing System
ASSU	Aviation Safety Systems Upgrade
ASTAB	Automated Status Board
ASW	Anti-Submarine Warfare
ATC	Air Traffic Control
ATC	Automated Technical Control
ATDLS	Advanced Tactical Data Link Systems
ATG	Afloat Tactical Group
ATIS	Advanced Technical Intelligence Support
ATIS	Advanced Technical Information System
ATM	Asynchronous Transfer Mode
ATO	Authority to Operate
ATO	Air Tasking Order
ATOCS	Air Tasking Order Compressed System
ATP	Advanced Tactical Planner
ATRC	Aegis Training and Readiness Center
AUTODIN	Automated Digital Network
AUTODIN	Automated Digital Information Network
AV3M	Aviation Maintenance Material Management

-- B --

B2CA	Bosnia Command and Control Augmentation
BAN	Base Area Network
BAR	Baseline Analysis Review
BARP	BF Analysis Review Panel
BBS	Baseband Switch
BCA	Broadcast Control Authority
BCST	Broadcast
BER	Bit Error Rate
BEST	Bandwidth Efficient Satellite Transport System
BEUI	BIOS Extended User Interface
BEWT	Battle Force Electronic Warfare Trainer
BF	Battle Force
BFAO	Battle Force Action Officer
BFEM	Battle Force Email
BF CCB	Battle Force Change Control Board
BFIN	Battle Force Information Network
BFIT	Battle Force Integration Team
BFO	Battle Force Officer
BFOSS	Battle Force Operational Sequencing

BFS Battle Force Superintendent  
 BFT Backfit Technical Review  
 BFTT Battle Force Tactical Training  
 BG Battle Group  
 BG CELL Battle Group Cellular  
 BGDBM Battle Group Data Base Management  
 BGSA Battle Group Systems Advisor(See FSET)  
 BGIT Battle Group Integration Team  
 BGIXS Battle Group Information Exchange System  
 BGPHEs Battle Group Passive Horizon Extension System  
 BIOS Basic Input/Output Systems  
 BISOG Blue in Support of Green  
 BIT Built-in Test  
 BLOS Beyond Line of Sight  
 BLII Base Level Information Infrastructure (now  
 ONE NET)  
 BM Beam Managed  
 BMCs Broadcast Management Centers  
 BMD Ballistic Missile Defense  
 BMTA Backbone Message Transfer Agent  
 BNIDS Basic Network and Information Distribution  
 Service  
 BNMC Bahrain Network Management Center  
 BOD Board of Directors  
 BOM Bill of Material  
 BPR Business Process Re-engineering  
 bps bits per second  
 BPSK Binary Phase Shift Keying  
 BRB Baseline Review Board  
 BRT Barrier Removal Teams  
 BTU Basic Terminal Unit  
 BUMED Bureau of Medicine  
 BUPERS Bureau of Naval Personnel  
 BW Bandwidth Management  
 BWS Bridge Work Station

## -- C --

C@S Collaboration At Sea  
 C&L Capabilities and Limitations  
 C2 Command and Control  
 C2I Command, Control and Intelligence  
 C2P Command and Control Processor  
 C2PC Command and Control PC  
 C2W Command and Control Warfare  
 C2WC Command and Control Warfare Commander  
 C2WCM Command and Control Warfare Commander's  
 Module  
 C3 Command, Control and Communications  
 C3F Commander Third Fleet  
 C3I Command, Control, Communications and  
 Intelligence  
 C4 Command, Control, Communications, and  
 Computers  
 C4I Command, Control, Communications, Computers,



and Intelligence

C5I Command, Control, Communications, Computers, Intelligence, and Combat Systems

C5IMP C5I Modernization Process

C4IFTW C4I For The Warrior

C4IMP C4I Modernization Plan

C4ISR Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

CA Certificate Authority

C&A Certification & Accreditation

CAC Common Access Card

CAW Certificate Authority Workstation

C&A Certification and Accreditation

CA Challenge Athena

CATS Consolidated Area Telephone System

CAC Common Access Card

CADRT Computer Aided Dead Reckoning Tracer

CAEMS Computer Aided Embarkation Management System

CAF Combat Air Forces

CAI Computer Aided Instruction

CAIII Challenge Athena III (Now CWSP)

CAINS Carrier Aircraft Inertial Navigation System

CALS Continuous Acquisition and Life Cycle Support

CANTRAC Catalog of Navy Training Courses

CAP Channel Access Protocol

CARTS CASREP ACTION RESPONSE TRACKING SYSTEM

CAS Call Accounting System

CASREP Casualty Report

CASS Centralized Aircraft Support System

CATCC Carrier Air Traffic Control Center

CATF Commander Amphibious Task Force

CBT Computer Based Training

CBI Computer Based Instruction

CC Combat Control

CCA Circuit Card Assembly

CCB Change Control Board

CCIB Configuration Control Interoperability Board Requirements Group

CCIP C4I Capabilities Implementation Plan

CCOP Cryptologic Carry-On Program

CCOI Critical Contact of Interest

CCSG Commander Carrier Strike Group (Formerly BG)

CCTV Closed Circuit Television

CDBS Central Data Base Server

CDC Combat Direction Center

CDD Capability Development Document

CDE Common Desktop Environment

CDF Combat Direction Finding

CDL Combat Data Link

CDL-N CDL-Navy

CDLMS Common Data Link Management System

CDLS Common Data Link System

CDMA Code Divisional Multiple Access

CDO	Command Duty Officer
CD ROM	Computer Disk, Read Only Memory
CDNU	Control Display Navigation Unit
CDSA	Combat Direction Support Activity
CDU	Control and Display Unit
CEA	Central Engineering Agent
CEC	Cooperative Engagement Capability
CEG	Communications Equipment Group
CENTRIXS	Combined Enterprise Regional Information Exchange System
CEO	Chief Executive Officer
CEPS	Communications Equipment Population Summary
CeTARS	Corporate Enterprise & Training Resource System
CEVI	Crypto Equipment Validation Information
CFCP	COTS Fleet Communication Package
CFE	CENTRIXS Four Eyes
CFFC	Command Fleet Force Commander
CFM:	Contractor Furnished Material
	<u>CFn Composeable FORCENet</u>
CFT	Cross Functional Teams
CG	Guided Missile Cruiser
CG MEF	Commanding General, Marine Expeditionary Force
CHBDL-ST	Common High Bandwidth Data Link - Surface Terminal
CHET	Combatant Homeport Engineering Team
CIA	Communications Information Advisory
CIB	Communications Information Bulletin
CIBS-M	Common Integrated Broadcast Service Modules
CID	Center for Information Dominance
CIDLS	Center for Information Dominance Learning Site
CIP	Critical Infrastructure Protection
CINC	Commander in Chief
CISN	Communications Information Systems and Networks
CISSP	Certified Information System Security Professional
CIWS	Close In Weapons System
CJTF	Commander Joint Task Force
CJCSI	Chairman of the Joint Chief of Staffs Manual
CLAN	Coalition Local Area Network
CLEW	Conventional Link 11 Waveform
CLIN	Contract Line Item Number
CLIP	Common Link Integration Processing
CM	Configuration Management
CMATT	CISN Management and Training Analysis
CMFP	Cooperative Maritime Forces Pacific
CMIO	COMSEC Material Issuing Officer
CMP	COE Message Processor
CMS	Career Management System
CMS	COMSEC Material System
CMSA	Cruise Missile Support Activity

CNAF	Commander Naval Air Force
CNAL	Commander Naval Air Force, Atlantic
CND	Computer Network Defense
CNDiD/BA	Computer Network Defense in Depth/Baseline Assessments
CNET	Chief of Naval Education and Training
CNFC	Combined Naval Forces CENTCOM
CNO	Chief of Naval Operations
CNSF	Commander Naval Surface Force
CNSL	Commander Naval Surface Force Atlantic
CNVA	Computer Network Vulnerability Assist
COBLU	Cooperative OUTBOARD Logistics Upgrade
COCOMS	Unified Combatant Command
CODS	Coalition Data Servers
COE	Common Operating Environment
COH	Complex Overhaul
COI	Contact of Interest
COI	Critical Operational Issue
COIN	Community of Interest Network
COMDAC	Command Display and Control
COMLANTFLT	Commander in Chief US Atlantic Fleet
COMMERSAT	Commercial Satellite
COMNAVSPACECOM	Commander, Naval Space Command (Now Naval Network and Space Operations Command -see NNSOC)
COMPACFLT	Commander in Chief US Pacific Fleet
COMPOSE	Common PC Operating Systems Environment
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
COOL	Credentialing Opportunities On-line
COP	Common Operational Picture
COP	Configuration Overhaul Planning
COR	Contracting Officer Representative
CORN	Change Order Request Notification
COSAL	Coordinated Shipboard Allowance List
COTS	Commercial Off the Shelf
COWAN	Coalition Wide-Area Network
CPG	Configuration Planning Group
CPG	Computer Processor Group
CPL	Certified Parts List
CPM	Centrally Provided Material
CPM	Command Product Matrix
CPF	Commander in Chief, Pacific Fleet
CPU	Central Processing Units
CR	Configuration Request
CRD	Capstone Requirements Document
CRIU	Channel Access Protocol Router Interface Unit
CRL	Certification Revocation List
CRLCMP	Computer Resources Life Cycle Management Plan
CRMA	Collection Requirements Management Application

CRT	Cathode Ray Tube
CRWG	Copernicus Requirements Working Group
CRIU	Router Interface Unit
CSAR	Combat Search and Rescue
CSD	Consolidated Software Deliveries
CSD	Communication at Speed and Depth
CSDTS	Common Shipboard Data Terminal Set
CSEL	Combat Survivor Evader Locator
CSFTL/P	Commander Strike Force Training Atlantic/Pacific
CSG	Carrier Strike Group
CSMP	Current Ships Maintenance Project
CSRR	Commercial SATCOM Regional Representative
CSRR	Common Submarine Radio Room
CST	COP Sync Tools
CSU	COP Sync Tools
CSU	Channel Switch Unit
CSP	Commercial SATCOM Program
CSDTS	Common Shipboard Data Terminal Set
CSEDS	Combat Systems Engineering and Development Station
CSEL	Combat Survivor Evader Locator
CSG	Carrier Strike Group
CSIT	Combat System Integration Testing
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CSO	Combat Systems Office
CSOSS	Combats Systems Operational Sequencing System
CSRR	Combat System Readiness Review
CSS	Communications Support System
CSU	Clock Stabilization Unit
CTAPS	Contingency Theater Automated Planning System (Now TBMCS)
CTO	Computer Tasking Orders
CTP	Common Tactical Picture (See COP)
CTT/HR	Commanders Tactical Terminal/Hybrid Receive Only
CUB	Cryptologic Unified Build
CUDIXS	Common User Digital Information Exchange Subsystem
CV/CVN	Aircraft Carrier/Aircraft Carrier (Nuclear)
CVBG	Carrier Battle Group
CVNS	Carrier Navigation System
CVIC	Aircraft Carrier Intelligence Center
CW	Continuous Wave
CWID	Coalition Warrior Interoperability Demonstration (Formerly JWID).
CWSP	Commercial Wideband SATCOM Program
C2/MC2	Milstar Uplink
C3/MC3	Milstar Downlink

## - D -

DAA Designated Approval Authority  
 DAB Defense Acquisition Board  
 DAGR Defense Advanced GPS Receiver  
 DAMA Demand Assigned Multiple Access  
 DAT Digital Audio Tape  
 DB Decibel  
 DBSS Direct Broadcast Satellite Service  
 DBU DMS Business Utility  
 DCE Data Communications Equipment  
 DCD Decision Centered Design  
 DCGS-N Distributed Common Ground Station-Navy  
 DCM Drydock Continuous Maintenance  
 DCP Department of the Navy Control Points  
 DCS Defense Communications System  
 DCS Display Control Subsystem  
 DD Destroyer  
 DDG Guided Missile Destroyer  
 DDN Defense Data Network  
 DDS Digital Data Set  
 DDRT Digital Dead Reckoning Tracer  
 DECM Decoy Electronic Countermeasures  
 DED Dead Availability  
 DEERS Defense Eligibility Enrollment System  
 DEP Distributed Engineering Plant  
 DESRON Destroyer Squadron  
 DF Direction Finding  
 DFAS Defense Finance and Accounting System  
 DFAX Direct-dial Facsimile  
 DGSIT Deploying Group Systems Integration Testing  
 DGAR Defense Advanced GPS Receiver  
 DGB Design Guidance Baseline  
 DHCP Dynamic Host Configuration Protocol  
 DIACAP Defense Information Assurance Certification  
 and Accreditation Program  
 DII Defense Information Infrastructure  
 DIWS-A Digital Imagery Workstation Suite Afloat  
 DIN Defense Intelligence Network  
 DISA Defense Information Systems Agency  
 DISN Defense Information System Network  
 DITSCAP Defense Information Technology Security  
 Certification and Accreditation Process  
 DITCO Defense Information Technology Contracting  
 Organization  
 DL Depot Level  
 DLT Digital Line Tape  
 DMA Defense Mapping Agency  
 DMP Depot Modernization Period  
 DMR Digital Modular Radio  
 DMS Defense Message System  
 DMSP Defense Meteorological Satellite Program  
 DNC Digital Nautical Charts  
 DNL Dual Net Link  
 DNP Dual Net Processor

DNS	Domain Name Server
DoD	Department of Defense
DODCP	Department of Defense Control Points
DODIIS	Department of Defense Intelligence Information System
DON	Department of the Navy
DOS	Disk Operating System
DPS	Digital Products Server
DRPM	Direct Reporting Program Managers
DRSN	Defense Red Switched Network
DS	Distance Support
DSA	Directory Service Agent
DSA	Design Services Allocation
DSA	Directory System Agent
DSCS	Defense Satellite Communications System
DSIU	Dual SINCGARS interface Unit
DSL	Digital Subscriber Line
DSN	Defense System Network
DSN	Defense Switched Network
DSP	Digital Signal Processor
DSP	DMS Service Provider
DSP	Deployables Support Plan
DSU	Digital Switching Unit
DSVL	Doppler Sonar Velocity Log
DSVT	Digital Secure Voice Terminal
DTD	Data Transfer Device
DT&E	Development Test & Evaluation
DTE	Data Terminal Equipment
DTED	Digital Terrain Elevation Data
DTH	Defense Transition Hub
DT/OT	Development Test/Operational Test
DTR	Data Terminal Ready
DTS	Data Terminal Set
DTTS	Digital Tracking and Trunking Switching
DTTS	Digital Tactical Telephone Switches
DUCA	Distributed User Coverage Area
DUSC	Directory User Service Center
DWT	Deep Water Trunk
DWTS	Digital Wideband Transmission System

-- E --

E3	Electromagnetic Environmental Effects
EADS	Expeditionary Air Defense System
EC5G	Expeditionary Command & Control, Communications, Computers, Combat Systems Grid
EC	Earth Coverage
EC	Enabling Capability
EC	Engineering Changes
eCCB	Electronic Change Control Board
ECCM	Electronic Counter Countermeasures
ECDIS-N	Electronic Chart Display and Information

## Systems - Navy

ECMU	Extended Core Memory Core Unit
ECP	Engineering Change Proposal
ECRC	Expeditionary Combat Readiness Center
ECRNOC	European Central Region Network Operating Center
ECS	Exterior Communications System
ECU	End Cryptographic Equipment
EDD	Estimated Delivery Date
EDM	Engineering Development Model
EDO	Engineering Duty Officer
EDSRA	Extended Drydocking Selected Restricted Availability
EELV	Evolved Expendable Launch Vehicle
EFW	Embedded Firewall
EHF	Extremely High Frequency (30-300 GHz)
EHF MDR	Extremely High Frequency, Medium Data Rate
EIP	Embeddable Infosec Product
EIP	Enterprise Information Portal
EIRP	Effective Isotropic Radiated Power
E JNL	Electronic JTIDS Network Library
EKMS	Electronic Key Management System
ELF	Extra Low Frequency
ELINT	Electronics Intelligence
EMC	Electromagnetic Compatibility
EMCON	Emission Control
EMI	Electro Magnetic Interference
EMP	Electro Magnetic Pulse
EMS	Element Management System
EMSS	Enhanced Mobile Satellite Service (IRIDIUM)
eNTRS	Enterprise Naval Training Reservation System
ENTSG	Enterprise Strike Group
ENWGS	Enhanced Naval War Gaming System
EOA	End Of Availability
EOB	Electronic Order of Battle
EOD	Explosive Ordnance Disposal
EOL	End of Life
EPLRS	Enhanced Position Location Reporting System
ERDB	Emerging Requirements Data Base
ERNOC	Element Management System
ERP	Enterprise and Resource Planning
ESD	Electrostatic Discharge
ESF	Expeditionary Security Force
ESG	Expeditionary Strike Group
ESIT	Embarkable Staff Integration Teams
ESM	Electronic Support Measures
ESPG	Embedded System Processor Group
ESRA	Extended Ship Restricted Availability
ETEC	End-to-End Capability
ETEPP	Electronic Tomahawk Employment Planning Package
ETCS	Expeditionary Tactical Communication System
ETT	Expeditionary Training Team
EURCENT	Central Europe

EVP Enhanced Verdin Processor  
 EVS Enhanced Verdin System  
 EW Electronic Warfare

-- F --

FAM Fleet Advisory Message  
 FAOE Fleet Air/Ocean Equipment  
 FAS Fleet Application Servers  
 FAT Fly Away Team  
 FBC Final Baseline Configuration  
 FBC Functional Baseline Configuration  
 FBE Fleet Battle Experiment  
 FC Field Changes  
 FCC Federal Communications Commission  
 FCCL FORCENet Compliance Check List  
 FCIP Field Change Improvement Program  
 FCP Fleet Communications Package  
 FDDI Fiber Data Distributed Interface  
 FDRR Fleet Delivery Readiness Review  
 FDRR Final Deployment Readiness Review  
 FDMA Frequency Division Multiple Access  
 FDNF Forward Deployed Naval Forces  
 FDRR Fleet Delivery Readiness Review  
 FDS Fixed Distribution System  
 FEC Forward Error Correction  
 FEP FLTSAT EHF Package  
 FFC Fleet Forces Command  
 FFG Guided Missile Frigate  
 FIBL FORCENet Implementation Baseline  
 FID Functional Interface Diagram  
 FIFO First In First Out  
 FIN Functional Identification Number  
 FIPS Federal Information Processing Standard  
 FIWC Fleet Information Warfare Center  
 FIST Fleet Imagery Support Terminal  
 FIT Final Integration Testing  
 FLEETEX Fleet Exercise  
 FLTCINC Fleet Commander-in-Chief  
 FLTSAT Fleet Satellites  
 FLT CON Fleet Network Operating Center  
 FM Frequency Modulation  
 FMX Fleet Messaging Exchange  
 FMAV Fleet Modernization Availability  
 FMP Fleet Modernization Program  
 FMP Field Management Plan  
 FMPMIS Fleet Modernization Program Management  
 Information System  
 FMS Foreign Military Sales  
 FMX Fleet Message Exchange  
 FNBBDT Future Narrow Band Digital Terminal  
 FnM Force Net Matrix  
 FNMOC Fleet Numerical METOC Center  
 FOT Follow-On Terminal



FOUO	For Official Use Only
FRCB	Fleet Readiness Certification Board
FRP	Fleet Response Plan or Fleet Readiness Program
FRPA	Fixed Reception Pattern Antenna
FSB	Fleet Support Broadcast
FSD	Fleet Support Detachment
FSET	Fleet Systems Engineering Team
FSK	Frequency Shift Keying
FSM	Food Service Management
FSM	Fleet SIPRNET Messaging
FTP	File Transfer Protocol
FTSC	Fleet Technical Support Center
FTSR	Feeder Telephone Service Request
FTP	File Transfer Protocol
FTSC	Fleet Technical Support Center (Lant/Pac)
FUNC	FORCENet Universal Needs Catalogue
FW	Firewall
FY	Fiscal Year
FYDP	Fiscal Year Defense Plan
FYOH	Fiscal Year of Overhaul
FYPR	Fiscal Year Programmed

-- G --

GALA	Global Average Line-of Sight Availability
GALE	Generic Area Limitation Environment
GATM	Global Air Traffic Management
GBS	Global Broadcast Service
GCBS	Ground Control Bombing System
GCCS	Global Command and Control System
GCCS-M	Global Command and Control System-Maritime
GCSS	Global Combat Support System
GCF	Garrison Communication Facility
GCTF	Global Counter-Terrorism Task Force
GDSC	Global Distance Support Center
GENSER	General Service
GEMIII	Global Engineering Methods Initiative for Integration and Interoperability
GFCP	Generic Front End Communications Processor
GFCS	Gun Fire Control System
GFE	Government Furnished Equipment
GFM	Government Furnished Material
GFO	GEOSAT Follow-on Satellite
GHZ	Gigahertz
GIG	Global Information Grid
GIG-E	Gigabit Ethernet
GINA	GPS Inertial Navigation Assembly
GMDSS	Global Marine Distress and Safety Service
GMF	Ground Mobile Force
GNFPP	Global Naval Forward Presence Policy
GNO	Global Network Operations
GNOSC	Global Network Operations System Center

GOBI	General Officer Bright Idea
GOES	Geo-stationary Operational Environmental Satellite
GOGO	Government Owned Government Operated
GOTS	Government Off-The-Shelf
G&PP	Guidance and Policy Paper
GPETE	General Purpose Electronic Test Equipment
GPS	Global Positioning System
GRAM	GPS Receiver Application Module
GRU	Gridlock Reference Unit
GSM	Global System for Mobile Communication
GUI	Graphic User Interface
GWOT	Global War on Terrorism

-- H --

HAG	High Assurance Guard
HAWK	Homing All the Way Killer
HAZMAT	Hazardous Materials
HCI	Human-Computer Interface
HDR	High Data Rate
HF	High Frequency (3-30 MHz)
HFDS	High Frequency Data System
HFRG	High Frequency Radio Group
HHR	High Hop Rate
HHST	Hand Held Satellite Terminal
HI	Horizontal Integration
HICOM	High Command
HIDS	Host Based Intrusion Detection System
HITS	Hostile Force Integrated Subsystem
HM&E	Hull Mechanical and Engineering
HP	Hewlett-Packard
HPA	High Powered Amplifier
HQ	Headquarters
HQMC	Headquarters Marine Corps
HSBCA	High Speed Buoyant Cable Antenna
HSD	High Speed Data
HSFB	High Speed Fleet Broadcast
HSGR	High Speed Global Ring
HSI	Human Systems Interface
HSSI	High Speed Serial Interface
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol
HVAC	Heating, Ventilation and Air Conditioning
HW	Hardware
HYDRA	Hierarchical Yet Dynamic Radio Architecture

-- I --

IA	Information Assurance
IA	Installing Activity
I&A	Identification and Authentication
I&W	Indications and Warning
IAAW	Information Assurance Assist Visit
IACS	Integrated Acoustic Communications System

IAS	Intelligence Analysis System
IASM	Intelligent Agent Security Module
IAT	Information Assurance Technician
IATO	Initial Authority to Operate
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IBC	Initial Baseline Configuration
IBFT	Integrated Battle Force Training
IBR	Initial Baseline Review
IBS	Integrated Bridge System
IC	Interior Communications
ICAS	Integrated Condition Assessment System
ICD	Installation Control Drawing
ICD	Installation Change Drawing
ICDB	Integrated Communications Data Base
ICE	Integrated Cooperative Engagement
ICO	Interface Control Officer
ICSTF	Integrated Combat System Test Facility
ICW	Interactive Course Ware
IDS	Intrusion Detection System
IDTC	Inter-Deployment Training Cycle
IO	Information Operations
I/O	Input/Output
ICOM	Integrated COMSEC
IDB	Intelligence Database
IDB	Installation Database
IDB	Integrated Data Base
IDCP	Intra-ARG Distributed Collaborative Planning
IDM	Information Dissemination Management
IDRS	Inter Deployment Readiness Cycle
IDS	Intrusion Detection Systems
IETM	Interactive Electronic Tech Manual
IFF	Identification, Friend or Foe
ILS	Integrated Logistics Support
ILSMP	Integrated Logistic Support Management Plan
ILSP	Integrated Logistics Support Plan
IM	Incidental Material
IMA	Intermediate Maintenance Activity
IMAV	Intermediate Maintenance Availability
IMO	Installation Management Office
IMI	Intermodulation Interference
IMINT	Imagery Intelligence
IMPACTS	IW Mission Planning, Analysis, and C2 Targeting System
INE	In Line Network Encryptor
INFOSEC	Information Security
INM	Integrate Network Management
INMARSAT	International Maritime Satellite
INS	Inertial Navigation System
INTELSAT	Intelligent Satellite
IO	Information Operations
IOC	Initial Operating Capability
IORNOC	Indian Ocean Regional Network Operating

Center

IP Internet Protocol  
 IPGPS Interim Portable GPS  
 IPR In Process Review  
 IPT Integrated Product Team  
 IPv6 Internet Protocol Version 6  
 IPX Internet Packet Exchange  
 IR Instruction Report  
 IRC Internet Relay Chat  
 IS INTELSAT Satellite  
 ISAR Inverse Synthetic Aperture Radar  
 ISB Independent Side Band  
 ISDN Integrated Services Digital Network  
 ISDS Information Screening & Delivery Subsystem  
 ISEA In-Service Engineering Agent  
 ISIC Immediate Superior in Command  
 ISM Information System Maintenance  
 ISM Iridium Secure Module  
 ISNS Integrated Shipboard Network System  
 ISO International Standardization Organization  
 ISP Internet Service Provider  
 ISP Inside Cable Plant  
 ISR Intelligence Surveillance & Reconnaissance  
 ISRAT Integration C4I Installation Synchronization  
 And Realignment Action Team(Carrier, Ship and  
 Shore)

IAM Information Assurance Manager  
 IAO Information Assurance Officer  
 IT Information Technology  
 IT-21 Information Technology for the 21st Century  
 ITAC Information Technical Assistance Center  
 ITAWDS Integrated Tactical Amphibious Warfare Data  
 System

ITC Information Technology Center  
 ITO Integrated Tasking Order  
 ITOC Integrated Technology Outreach Center  
 ITP Integrated Terminal Programs  
 ITSS Information Technology Support Center  
 IUSS Integrated Undersea Surveillance System  
 IVCS Integrated Voice Communications System  
 IVS Integrated Video System  
 IW Information Warfare  
 IXS Information Exchange Subsystem

-- J --

JATACS JDISS Advanced Tactical Cryptologic Support  
 JBS Joint Broadcast Service  
 JCA JSIPS Concentrator Architecture  
 JCALS Joint Computer-aided Logistics and Support  
 Systems  
 JCDX Joint Cross Domain Exchange  
 JCMPO Joint Cruise Missile Project Office  
 JCF Justification Cost Form

JCS Joint Chiefs of Staff  
 JDISS Joint Deployable Intelligence Support System  
 JDMS Joint Data Management Systems  
 JEAP Joint Electronic Analysis Program  
 JETS JMCIS Expedited Text Search  
 JFACC Joint Forces Air Component Commander  
 JFMCC Joint Forces Maritime Component Commander  
 JFMM Joint Fleet Maintenance Manual  
 JFN Joint Forces Network  
 JFTOC Joint Fleet Telecommunications Operating  
 Center  
 JIC Joint Intelligence Center  
 JICO Joint Interface Control Officer  
 JICF Joint Integrated Communications Facility  
 JINTACCS Joint Interoperability Tactical Command and  
 Control Systems  
 JIST Joint Integrated Systems Technology  
 JMAST Joint Mobile Ashore Support Terminal  
 JMCIS Joint Maritime Command Information System  
 (Note: No longer utilized - reference only)  
 JMCIS-A Joint Maritime Command Information System -  
 Afloat  
 JMCOMS Joint Maritime Communications System  
 JMHS Joint Message Handling System  
 JMINI Joint MILSATCOM Network Integrated Control  
 System  
 JMIO Joint Maritime Information Operations  
 JMTCSS Joint Maritime Tactical Communications  
 Switching System  
 JNL Joint Network Library  
 JOC Joint Operations Center  
 JOCC Joint Operations Command Center  
 JOPES Joint Operational Planning and Execution  
 System  
 JOTS Joint Operations Tactical System  
 JPO Joint Program Office  
 JPALS Joint Precision Approach and Landing  
 JPMO Joint Program Management Office  
 JRE Joint Range Extension Program  
 JROC Joint Requirements Oversight Council  
 JSTARS Joint Surveillance Target Attack Radar System  
 JSIPS-N Joint Service Imagery Processing System -  
 Navy  
 JSN Job Sequence Number  
 JTF Joint Task Force  
 JTFEX Joint Task Force Exercise  
 JTG Joint Task Group  
 JTIDS Joint Tactical Information Distribution  
 System  
 JTRS Joint Tactical Radio System  
 JTT Joint Tactical Terminal  
 JU JTIDS Units  
 JWID Joint Warrior Interoperability Demonstration

JWICS (Now referred to as CWID)  
Joint Worldwide Intelligence Communications  
System

-- K --

kbps kilobits per second  
KEYMAT Key Material  
kHz Kilohertz  
KL KLEIGLIGHT  
KP Key Processor  
KU Frequency at SHF  
KWEB Knowledge Web

-- L --

LAAS Local Area Augmentation System  
LAC Launch Area Coordinator  
LAN Local Area Network  
LANE LAN Emulation  
LAR Liaison Action Record  
LAWS Land Attack Warfare System  
LCC Amphibious Command Ship  
LCM Life Cycle Manger  
LCMS Learning Content Management System  
LDR Low Data Rate  
LDSA Local Director System Agent  
LCM Leased Channel Mode  
LEDS Link 11 Display System  
LEO Low Earth Orbit  
LES Land Earth Station  
LF Landing Force  
LF Low Frequency (30-300 kHz)  
LHA/LHD Amphibious Assault Ship (General Purpose)  
LHR Low Hop Rate  
LK-4A TADIL C  
LK-11 TADIL A  
LK-16 TADIL J  
LLFA Low Low Frequency Array  
LLTM Long Lead Time Material  
LMC Link Monitoring Capability  
LMD Local Management Device  
LMS Learning Management System  
LMS Local Monitor Station  
LNA Low Noise Amplifier  
LNB Low Noise Block  
LOB Line-of-Bearing  
LOCE Linked Ops Intell Center Europe  
LOGCOP Logistics Common Operating Picture  
LOS Line of Sight  
LPD Low Probability of Detection  
LPI Low Probability of Intercept  
LPI/D Low Probability of Intercept/Detection  
LPM Locally Provided Material

LPRU           Lowest Possible Replacement Unit  
 LRA            Local Registration Authority  
 LRIP           Low Rate Initial Production  
 LRU            Lowest Replaceable Unit  
 LSB            Lower Side Band  
 LSD            Large Screen Display  
 LWCA           Light Weight Communications Antenna

-- M --

MAD            Magnet Anomaly Detector  
 MAGR           Miniaturized Airborne GPS Receiver  
 MAGTF          Marine Air Ground Task Force  
 MALS           Marine Aviation Logistics Squadrons  
 MAN            Metropolitan Area Network  
 MARCEMP        Manual Relay Center Modernization Program  
 MARCORSYSCOM   Marine Corps Systems Command  
 MARMC          Mid Atlantic Regional Maintenance Center  
 MAST           Mobile Ashore Support Terminal  
 Mbps           Megabits per second  
 MCAG           Maritime Civil Affairs Group  
 MCAP           Medium-Rate Channel Access Protocol  
 MCCR           Mission Critical Computer Resources  
 MCFI           Multi-Coalition Forces Iraq  
 MCP            Multi Channel Patch Panel  
 MCPT-1         MILSTAR Communications Planning Tool-  
                   Integrated  
 MCU            Multi-Point Control Units  
 MCIXS          Maritime Cellular Information Exchange System  
 MCMRON         Mine Counter Measures Squadron  
 MCNOC          MARCORSYSCOM Network Operations Center  
 MC             Marine Corp  
 MCS            Message Conversion System  
 MCS            Multi Functional Cryptologic Systems  
 MCSE           Microsoft Certified Systems Engineer  
 MCTN           Marine Corp Telecommunications Network  
 MCTSSA         Marine Corp Tactical Systems Support        Activity  
 MDA            Milestone Decision Authority  
 MDEP           Milstar/DISN Entry Point  
 MDDS           Mission Data Display System  
 MDR            Medium Data Rate  
 MDS            Mission Display System  
 MDU            Mission Data Update  
 MEF            Marine Expeditionary Force  
 MEF            Middle East Force  
 MEFSAG         Middle East Force Surface Action  
 MEDAL          Mine Warfare Decision Aids Library  
 METMF          Meteorological Mobile Facility  
 MetOc          Meteorology and Oceanography  
 MEU            Marine Expeditionary Unit  
 METOC          Meteorological and Oceanographic  
 MF             Medium Frequency  
 MFI            Multi Function Interpreter

MFL	Multi-Frequency Link
MFU	Message Forwarding Utility
MFU	Mission Folder Update
MOC	Maritime Operations Center
MHQ	Maritime Headquarters
MHz	Megahertz
MICFAC	Mobile Integrated Communications Facility
MIDB	Modern Integrated Data Base
MIDS	Multi-Functional Distribution System
MILSPEC	Military Specification
MILSATCOM	Military Satellite Communications
MILSTAR	Military Strategic and Tactical Relay
MIL STD	Military Standard
MILSTRIP	Military Standard Requisitioning and Issue Procedure
MINI DAMA	Miniaturized Demand Assigned Multiple Access
MINI NOC	Miniature Network Operation Center
MISREP	Mission Report
MITE	Monthly Inport TADIL Exercise
MITT	Maritime Integrated Tailored Training
MIUW	Mobile Inshore Undersea Warfare
MIWRG	Mine Warfare Readiness Group
MLA	Mail List Agent
MLDN	Maritime Logistics Data Network
MLP	Multi-Function Precedence Preemption
MLS	Multi-Level Security
MMG	Mast Mechanical Group
MOA	Memorandum of Agreement
MOCC	Mobile Operations Command Center
MOSPF	Multicast Open Shortest Path First
MOU	Memorandum of Understanding
MPEG	Moving Picture Expert Group
MPT	Manpower, Personnel and Training
MRMS	Maintenance Resource Management System
MROC	Multi-Command Required Operational Capability
MRS	Mini Rawinsonde System
MSC	Military Sealift Command
MSD	Material Support Date
MSE	Mobile Subscriber Equipment
MSEL	Master Scenario Event List
MSKC	MetOc Systems Knowledge Center
MSL	Multi-Security Level
MSOC	Milstar Satellite Operations Center
MSP	Message Security Protocol
MSS	Multiple Subscriber Service
MSS	Mobile Satellite Service
MSS	Multi-Protocol Switch Server
MSWG	USMC Wing Support Groups
MTA	Message Transfer Agent
MTC	Multi Tadil Capability
MTP	Multi Tadil Processor
MTT	Mobile Training Team
MUOS	
MWSS	USMC Wing Support Squadrons



-- N --

1NCD	First Naval Construction Division
NACC	Next Generation ARG Collaboration Capability
NADGE	NATO Air Defense Ground Environment
NALCOMIS	Naval Aviation Logistics Command Management Information System
NALCOMIS IMA	NALCOMIS Intermediate Maintenance Activities
NALCOMIS OMA	NALCOMIS Organizational Maintenance Activities
NALDA	Naval Aviation Logistics Data Analysis
NAN	Navy Afloat Networks
NAS	Naval Air Station
NAT IPT	Naval Afloat/Targeting Integrated Process Team
NATO	North Atlantic Treaty Organization
NAVAIRSYSCOM	Naval Air Systems Command
NCDOC	Naval Computer Incident Response Team
NAVICP	Navy Inventory Control Point
NAVCOMPT	Comptroller of the Navy
NAVELSG	Navy Expeditionary Logistics Support Group
NAVFLIRS	Naval Aviation Flight Records
NAVMEDIACEN	Naval Medical Center
NAVMACS	Navy Modular Automated Communications System
NAVNEWS	Naval News
NAVOCEANO	Naval Oceanographic Office
NAVSUP	Naval Supply Systems Command
NAVSEA	Naval Sea Systems Command
NAVSTAR GPS	Navigation Satellite Timing and Ranging System GPS
NAVSSI	Navigation Sensor System Interface
NAVSUP	Naval Supply Systems Command
NAVTEX	Navigation Telex
NCDOC	Navy Cyber Defense Operations Command
NCTAMS	Naval Computer and Telecommunications Area Master Station
NCSS	Naval Combat Support System
NCS	Net Control Station
NCTS	Naval Computer and Telecommunications Station
NCTSI	Navy Center for Tactical Systems Interoperability
NCVI	Navy Certificate Validation Infrastructure
NCW	Naval Coastal Warfare
NCW	Netcentric Warfare
NDE	Navy Data Environment
NCT	Net Cycle Time
NDI	Non Developmental Item
NECC	Naval Expeditionary Combat Command
NECC	Navy EHF Communications Controller
NECOS	Net Control Station
NECSS	Naval Electronic Combat Surveillance System

NES	Network Encryption System
NESP	Navy EHF Satellite Communications Program
NETC	Navel Education and Training Command
NETBEUI	NETBIOS Extended User Interface Protocols
NETBIOS	Network Basic Input/Output System Protocols
NETC	Navy Education and Training Command
NAVNETWARCOM	Naval Network Warfare Command
NEXRAD PUP	Next Generation Radar Principal User Processors
NFC	Numbered Fleet Commander
NFN	Naval Fires Network
NGCR	Next Generation Computer Resources
NGN	Next Generation Network
NIAPS	Navy Integrated Applications Product Suite
NIAT	Navy Information Assurance Team
NIC	Network Interface Cards
NICC	Navy Integrated Call Center
NIDTS	NATO Initial Data Transfer System
NIF	Network Intrusion Filter
NIMA	National Imagery and Mapping Agency
NIIN	Navy Integrated Information Network
NIEWS	NTCS-A Imagery Exploitation Workstation
NILE	NATO Improved Link 11
NIMA	National Imagery Mapping Agency
NIPRNET	Non classified Internet Protocol Routing Network
NIPS	Navy Information Processing System
NIPS	NTCS-A Intelligence Processing Services
NISE	Navy In Service Engineering
NITDS	Nato Initial Data Transfer System
NITES	Navy Integrated Tactical Environmental Subsystem
NKDS	Navy Key Distribution System
NKMS	Navy Key Management System
NKO	Navy Knowledge Online
NLT	No Later Than
NMC	Network Management Center
NMCI	Navy-Marine Corp Intranet
NMIMC	Navy Medical Information Management Command
NMPS	Naval Mission Planning System (NMPS)
NNFE	Naval NETWAR/FORCEnet Enterprise
NNSOC	Naval Network and Space Operations Command
NNWC	Naval Network Warfare Command
NOC	Network Operating Center
NOFORN	No Foreign Nationals
NOS	Network Operating Systems
NOW	Navy Order Wire
NOWNET	Navy Order Wire Network
NRAD	Navy Research and Development
NRI	Net Radio Interfaces
NSA	National Security Agency
NSA	Naval Supply Activity
NSB	Narrow Spot Beam
NSC	Naval Supply Center

NSGA	Naval Security Group Activity
NSIPS	Navy Standard Integrated Personnel System
NSOM	Navy Systems Operational Manager
NSS	Navy Simulation System
NSS	New Skies Satellite
NSS	Network System Security
NST	Navy Standard Teleprinter
NSV	Noise, Shock and Vibration
NSVT	Network Security Vulnerability Technician
NSWC	Naval Surface Warfare Center
NT	New Technology
NTCS-A	Navy Tactical Command System - Afloat
NTCSS	Naval Tactical Command Support System
NTDS	Navy Tactical Data System
NTDPS	Non Tactical Data Processing System
NTIRA	Naval Tool for Interoperability and Risk Assessment
NTMPS	Navy Training Management Planning System
NTP	Navy Training Plan
NTR	Navy Technical Representative
NTS	Naval Telecommunications System
NTSP	Navy Training Systems Plan
NUWG	Network Users Working Group
-- O --	
OA	Operational Architecture
OA	Operational Assessment
OASIS	OTH-T Aircraft Sensor Interface System
OAT	Optional Application Tape
OBRP	On Board Repair Parts
OBT	On Board Training
OBU/OED	Ocean Surveillance Information System(OSIS) Baseline Upgrade/OSIS Evolutionary Development
OCONUS	Outside Continental United States
OCRS	Online Compliance Reporting System
OCSP	On-Line Certificate Status Protocol
OEM	Original Equipment Manufacturer
OIMA	Optimized Intermediate Maintenance Activities
OJT	On the Job Training
OMA	Organizational Maintenance Activity
OM-FTS	Operational Maneuver From the Sea
OM&N	Operations Maintenance - Navy
OMS	Ordnance Management System
OMMS	Organizational Maintenance Management System
ONE NET	Overseas Navy Enterprise Network (Replaces BLII)
ONI	Office of Naval Intelligence
ONR	Office of Naval Research
OOMA	Optimized Organizational Maintenance Activities
OEF	Operation Enduring Freedom
OOMA	Marine Air Logistics Squadron

OPEVAL	Operational Evaluation
OPN	Other Procurement Navy
OPS	Operations
OPTEVFOR	Operational; Test and Evaluation Force
OQPSK	Off Quadrature Phase Shift Keying
OR	Operational Requirement
ORD	Operational Requirements Document
ORDALT	Ordnance Alteration
ORTS	Operational Readiness Test System
OS	Operating System
OSI	Open System Interconnection
OSIS	Ocean Surveillance Information System
OSP	Outside Cable Plant
OSPF	Open Shortest Path First
OSS	Operations Support System
OTAR	Over The Air Rekeying
OTAT	Over The Air Transmission
OTCIXS	Officer in Tactical Command Information Exchange System
OTH-T	Over-the-Horizon Targeting
OTRR	Operational Test Readiness Review
OUTBOARD	Shipboard Acquisition and Direction Finding System

-- P --

P3I	Pre Planned Product Improvement
PABX	Private Automatic Branch Exchange
PACMEF	Pacific Middle East Force
PACOM	Pacific Command
PARM	Participating Managers
PBL	Performance Based Logistics
PBX	Private Branch Exchange
PC	Personal Computer
PCMT	Personal Computer Message Terminal
PCS	Personal Communications Service
PD	Periscope Depth
PD	Project Directive/Program Directorate
PDA	Personal Digital Assistant
PDR	Preliminary Design Review
PDU	Power Distribution Unit
PEO	Program Engineering Office
PERA	Planning and Engineering for Repairs and Alterations
PE	Program Engineering
PEO	Program Executive Office
PEOCMPANDUAV	PEO Cruise Missile Program and Unmanned Air Vehicle
PGM	Precision Guided Munitions
PGWS	Primary Group Ware Server
PHIBGRU	Amphibious Group
PHIBRON	Amphibious Squadron
PICT	Programmable Integrated Communications Terminal

PIDS	Personal Interface Devices
PIP	Primary Injection Point
PITCO	Pre Installation Test and Check Out
PJOCS	Pilot Joint Operation Command system
PK	Public Key
PKE	Public Key Enabling
PKI	Public Key Infrastructure
PLAD	Plain language Address Designator
PLGR	Precision Lightweight GPS Receiver
PLL	Phase Locked Loop[
PLRS	Position Location and Reporting System (USMC)
PLT	Passive Link Tap
PM	Program Manager
PMA	Phased Maintenance Availability
PMO	Program Management Office
PMW	Program Manager Warfare (SPAWAR)
PMINT	PHIBRON/MEU Integration
PNT	Position, Navigation and Timing
POA&M	Plan of Action & Milestones
POC	Point of Contact
POM	Program Objective Memorandum
PoP	Point of Presence
POR	Program of Record
POTS	Plain Old Telephone System
PPBS	Planning, Programming and Budgeting System
PPL	Preferred Products List
PPS	Precise Positioning Service
PRNOC	Pacific Region Network Operating Center
PSA	Post Shakedown Availability
PSK	Phase Shift Keying
PSTN	Public Switched Telecommunications Network
PTA	Precision Timing and Astronomy
PTP	Point-To-Point
PTW	Precision Targeting Workstation
PU	Participating Unit
PVT	Position, Velocity and Time
PY	Planning Yard

-- Q --

QA	Quality Assurance
QMCS	Quality Monitoring Control System
QMS	Quality Monitoring System
QOS	Quality of Service
QPL	Qualified Parts List
QPSK	Quadrature Phase Shift Keying
QRC	Quick Reaction Capability

-- R --

R&D	Research and Development
R&S	Routing and Switching
R&R	Roles and Responsibilities
RA	Registration Authority

RADDS	Radar Digital Distribution System
RAID	Redundant Array of Inexpensive Drives
RAPIDS	Real Time Automated Personnel Identification System
RAST	Recovery Assist Securing and Transverse System
RAV	Restricted Availability
RBS	Readiness Based Sparing
RCOH	Refueling Complex Overhaul
RCS	Radio Communications Subsystem
RCS	RADAR Cross Section
RDA	Research, Development, and Acquisition
RDD	Required Delivery Date
RDC	Rapid Deployment Capability
RDF	Radio Direction Finding
REM	Range Extension Model
REPEAT	Repeatable Performance Evaluation and Analysis Tool
RF	Radio Frequency
RITC	Regional Information Technology Center
RLAR	Reverse Liaison Action Record
RLGN	Ring Laser Gyro Navigator
RMA	Revolution in Military Affairs
RMC	Regional Maintenance Center (Replaced FTSC)
RMMCOC	Regional Maintenance And Modernization Coordination Office
RNOC	Regional Network Operating Centers
RNOSC	Regional Network Operations Security Center
ROC&POE	Required Operational Capability and Projected Operational Environment
ROH	Regular Overhaul
ROM	Read Only Memory
RPA	Receiver Pre-Amplifier
RSIM	
RTC	Remote Terminal Component
RTS	Real-Time Sub System

-- S --

SA	Situation Awareness
SAASM	Selective Availability Anti-Spoofing Module
SABER	Situational Awareness Beacon with Reply
SABRES	Ship Alteration Budget Reporting and Evaluation System
SACCS	Shipboard Automated Communication Control System
SADS	Submarine Antenna Distribution Systems
SAFENET	Survivable Adaptable Fiber Optic Embedded Network
SALTS	Streamlined Automated Logistics Transmission System
SAML	Security Assertion Markup Language
SAMS	Shipboard Automated Medical System
SAR	Search and Rescue

SAR	Satellite Access Requirement
SAR	Ship Alteration Record (Replaced by SCD)
SARTIS	Shipboard Advanced Radar Target Identification System
SAS	Shipboard Antenna System
SATCOM	Satellite Communications
SATNAV	Satellite Navigation
SBM	Satellite Broadcast Manager
SC21	Surface Combatants 21 Century
SC	Ship Check
SCAMP	Single Channel Anti- Jam Man portable
SCC	Sea Combat Commanders
SCCD	Ship Configuration Change Proposal
SCCP	Ships Configuration Change Proposal
SCD	Ship Change Document
SCI	Sensitive Compartmented Information
SCLISIS	Ship Configuration and Logistics Support Information System
SCN	Shipbuilding and Construction -Navy
SCONUM	Ships Control Number
SCSI	Small Computer System Interface
SCSS	Submarine Communications Support System
SD	San Diego
SDU	Satellite Direct User
SDB	Satellite Data Base
SELOR	Ships Emitter Location Report
SEMCIP	Shipboard Electro Magnetic Compatibility Improvement
SES	Ship Earth Stations
SFEWG	Strike Force Engineering Working Group
SGITR	Strike Group Interoperability Training Rep
SGLS	Space/Ground Link Subsystem
SGMTT	Strike Group Multi-TADIL Training
SGOT	Strike Group Oceanography Team
SGS/AC	Shipboard Gridlock System/Automatic Correlation
SHF	Super High Frequency (3-30 GHz)
SHIPALT	Ship Alteration
SI	Sensitive Information
SIAB	Snap-In-A-Box
SIC	SI Correlator
SID	Shipboard Installation Drawing
SIDE	SPAWAR Integrated Data Environment
SIGINT	Signals Intelligence
SIGSEC	Signal Security
SIM	Subscriber Identity Module
SINCGARS-SIP/ ASIP	Single-Channel Ground and Airborne Radio System - Systems Improvement Program/Advanced Systems Improvement Program
SIOC	Ship Information Operations Center
SIPRNET	Secret Internet Protocol Router Network
SITE	Shipboard Information Training and Entertainment
SITREP	Situation Report

SKED	Schedules (ships)
SLA	Service Level Agreement
SLEP	Service Life Extension Program
SLEW	Single Tone Link-11 Waveform
SLVR	Submarine LF/VLF VME Bus Receiver
SMART-T	Secure Mobile Anti-Jam Reliable Tactical Terminal
SMB	Submarine Message Buffer
SME	Subject Matter Expert
SMG	Secure Mail Guard
SMOOS	Shipboard Meteorological and Oceanographic Observation System
SMQ-11	Weather Satellite Receiving-Recording System
SMS	Skills Management System
SMS	Single Messaging Solution
SMTP	Simple Message Transfer Protocol
SNADIS	Submarine Non-Tactical Application Delivery Interface System
SNAP	Shipboard Non-tactical ADP Program
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ration
SOE	Schedule of Events
SOF	Special Operations Forces
SOI	Signals of Interest
SOMS	Shift Operations Maintenance System
SONET	Synchronous Optical Network
SOTA	Satellite Ocean Tactical Application
SOVT	Systems Operational Verification Test
SPARC	Scalable Processor Architecture
SPAWAR	Space and Naval Warfare Systems Command
SPM	Ship's Program Manager
SPX	Sequence Packet Exchange
SPRAC	Special Reporting and Coordination Net
SQL	Structured Query Language
SRA	Selected Restricted Availability
SRBM	Shipboard Receive Broadcast Manager
SRCS	Shore Remote Control System
SRGPS	Shipboard Relative Global Positioning System
SRK	Steady Receive Key
SRS	Shipboard Receive Suite
SSA	Software Support Activity
SSA	Solid State Amplifier
SSAA	System Security Authorization Agreement
SSB	Single Side Band
SSBN	Submersible, Ship, Ballistics, Nuclear (sub)
SSDS	Ship Self Defense System (ACDS follow-on)
SSC	SPAWAR Systems Center
SSE	Systems Security Engineering
SSEE	Ship Signal Exploitation Equipment
SSES	Ship Signal Exploitation Space
SSFA	SPAWAR Space Field Activity
SSGN	Submersible Ship, Guided, Nuclear (sub)
SSIL	Systems/Sub System Interface List
SSIXS	Submarine Satellite Information Exchange



	Subsystem
SSN	Navy Nuclear-powered (attack) Submarine
SSNS	Standard Supply Numbering System
SSO	Single Sign On
SSPA	Solid State Power Amplifier
SSS	System Supervisor Station
SSRBM	Sub-Surface Receive Broadcast Manager
SSRS	Sub-Surface Receive Suite
STAR	Standard Attribute Reference Manual
STARS	Standard Accounting and Recording System
STAR-T	SHF Tri-Band Advances Range Extension Terminal
STE	Secure Terminal Equipment
STU III	Secure Telephone Unit III
STP	Shielded Twisted Pair
STELLA	System to Estimate Latitude and Longitude Astronomically
STEP	Standardized Tactical Entry Point
STEP	Secure Telecommunications Entry Point
STICS	Scalable Transportable Intelligence Communications System
STIMS	Shipboard Tactical Information Management System
S-TRED	Standard Tactical Receive Equipment Display
STS	Secure Telephone System
STT	Shore Targeting Terminal
SUB HDR	Submarine High Data Rate
SURTASS	Surveillance Towed Array Sensor System
SVoIP	Secure Voice Over Internet Protocol
SVGA	Super Video Graphics Array
SW	Software
SWEDE	Sea Warrior Enterprise Data Environment
SWR	Supplemental Weather Radar
SWRMC	Southwest Regional Maintenance Center
SYSCOM	Systems Command

-- T --

T-1	1.544 Mbps
T-3	45 Mbps
T&C	Telemetry and Command
TAC	Tactical Advanced Computer
TACAN	Tactical Air Navigation
TACCIMS	Theater Automated Command and Control Information Management System
TACINTELL II	Tactical Intelligence Information Exchange System Phase II
TACS	Theater Air Control System (USAF)
TACTERM	Tactical Terminal
TAV	Technical Availability
TADIL	Tactical Data Information Link
TADIXS	Tactical Digital Information Exchange System/Subsystem
TAMD	Theater Air Missile Defense

TAMPS	Tactical Aircraft Mission Planning System
TARPS	Tactical Air Reconnaissance Pod System
TASS	TACTERM ANDVT Shore System
TAV	Technical Availability
TBD	To Be Determined
TBMCS	Theater Battle Management and Core System
TBMD	Theater Ballistic Missile Defense
TCD	Target Configuration Date
TCO	Tactical Combat Operations System
TCP	Transport Control Protocol
TCS	Tactical Cryptologic Systems
TD:	Technical Directive
TDA	Tactical Decision Aid
TDBM	Track Database Manager
TDL	Tactical Data Links
TDN	Tactical Data Network
TDMA	Time Division Multiple Access
T&E	Test and Evaluation
TEAMS	Tactical EA-6B Mission Support System
TEDS	Tactical Environmental Server
TELEPORT	Telecommunications Port
TEMPEST	Visual National Policy for the Control of Compromising Emanations
TEMPALT	Temporary Alteration
TEPP	Tomahawk Engagement Planning Package
TESS (3)	Tactical Environmental Support Systems (3)
TFDS	Time and Frequency Distribution System
TFTA	Tomahawk Fleet Training Aids
TDMA	Time Division Multiple Access
TDP	Tactical Data Processor
TEPEE	Tomahawk Engagement and Planning Exercise Evaluation
TES-N	Tactical Exploitation System-Navy
TESS	Tactical Environmental Support System
TFCC	Tactical Flag Command Center
TFW	Task Force Web
TGRS	Transportable Ground Receive Suite
THAAD	Theater High Altitude Area Defense
TIBS	Tactical Information Broadcast System
TIC	Tactical Information Coordinator
TIDS	Tactical Integrated Digital System
TIMS	Tactical Flag Command Center Information Management System
TIP	Theater Injection Point
TIP	TDMA Interface Process
TIS	Tactical Input Segment
TISS	Thermal Imaging Sensor System
TLAM	Tomahawk Land Attack Missile
TLS	Timeline Summary
TMG	Tactical Message Gateway
TMIP	Theater Medical Information Program
T-nT	Tactical-non-Tactical
TOPSCENE	Tactical Operations Preview Scene
TPS	Tomahawk Planning System

TRAP	Tactical Related Applications
TRE	Tactical Receive Equipment
TRDF	Transportable Radio Direction Finding System
TRIDENT IRR	Trident Integrated Radio Room
TRITAC	Tri-Service Tactical Communications
TRPPM	Training planning processes methodology
TRSS	Tactical Remote Sensor System
TRWS	TESS Remote Workstation
TSA	Training Situation Awareness
TSC	Tactical Support Center
TSIP	Telecommunications System Installation Plan
TSCM	Tactical Strike Coordination Module
TSS	Tactical Switching System
TSw	Tactical Switching
TS/SCI	Top Secret/Sensitive Compartmented Information
TSSS	Training Sim Stim System
TTC	Track-to-Track Correlator
TTE	Tactical Training Equipment
TTGP	Tactical Training Group Pacific
TTRAMS	Trouble Ticket Reporting Analysis and Metrics System
TTY	Teletype
TV-DTS	Television Direct to Sailors
TVRO	Television Receive Only
TVS	Tactical Variant Switch
TWCS	Tomahawk Weapons Control System
TYCOM	Type Commander

-- U --

U2	Uniform Automated Data Processing System-SP2
UARNOC	United Atlantic Regional NOC
UA	User agent
UAV	Unmanned Aerial Vehicle
UB	Unified Build
UDP	User Datagram Protocol
UFO	UHF Follow-On
UFO/E	UFO/EHF
UFO/EE	UHF Follow-on Enhanced EHF
UHF	Ultra High Frequency (300-3000Mhz)
UIC	Unit Identification Code
UK	United Kingdom
ULSS	User Logistic Support Summary
UPS	Un-interruptible Power Supply
USA	United States Army
USAF	United States Air Force
USB	Upper Side Band
USCG	United States Coast Guard
USMC	United States Marine Corps
USMTF	United States Message Text Format
USN	United States Navy
UTP	Unshielded Twisted Pair

## -- V --

5VM	Five Vector Model
VAAP	Vulnerability Analysis and Assistance Program
VCNO	Vice Chief of Naval Operations
VEIL	Variable Encryption and Intelligence Labeling
VHF	Very High Frequency (30-300 MHz)
VIG	Video Interface Group
VIP	Video-switch Interface Package
VIXS	Video Information Exchange System
VLAN	Virtual LAN
VLF	Very Low Frequency (3-30 kHz)
VME	Versus Module Europa
VMS	Voyage Management System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VSRR	VINSON Shore Radio Remote
VSRT	VINSON Shore Radio Terminal
VTC	Video Teleconferencing
VVFDT	Video Voice Facsimile/Data Terminal

## -- W --

WAN	Wide Area Network
WAPS	Wireless Access Points
WAAS	Wide Area Augmentation System
WDC	Work Definition Conference
WEB ATIS	Web Automated Technical Information System
WECAN	Web Centric ASW Net
WGS	Wideband Gapfiller Satellite
WGS	Wideband Global System
WINS	Windows Internet Name Service Protocol
WMT	Waterfront Maintenance Teams
WOO	Window of Opportunity
WSF	Work Station Function
WSV	Weapons Systems Video
WWMCCS	World Wide Military Command and Control System
WWW	World Wide Web

## -- X --

X-DECK	Cross Deck
--------	------------

## -- Y--

Y2K	Year 2000
-----	-----------

## CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

**APPENDIX B**  
**COMSPOT REPORTING**

Communications Spot (COMSPOT) reports will be submitted by all ships and shore facilities at any time communication outages or degradations are encountered. Submit the COMSPOT to the servicing NCTAMS and communications station respectively, info to the appropriate numbered fleet commander and ISIC. Timely submissions of COMSPOT reports are required, within thirty minutes of outage. Updates will be provided every hour or upon significant change in status. If systems can not be restored within 48 hours, submission of a CASREP will be sent in accordance with Joint Force Maintenance Manual. Do not delay CASREP submission because the cause of the outage is unclear (e.g., transport versus network). Intermittent outages should be considered for CASREP as well once the troubleshooting has exceeded the 48 hour window. The following COMSPOT report will be used by all units:

COMSPOT drafters will adhere to the following:

- Use the CNO mandated message drafting application Common Message Processor (CMP).
- Ensure the MSGID is listed as "COMSPOT" and is followed by the units name. For example, USS Theodore Roosevelt will be entered as "Theodore Roosevelt". Ensure proper use of serial numbers, and indicate if initial, update or final.
- Ensure the COMEV field is presented as a date time group value. For example, if a circuit goes down at 0101Z on 01 December, enter it as "010101ZDEC07". Ensure that log up times are entered in the same way, (i.e.,: "COMEV/OTG/010101ZDEC07/010203ZDEC07//". If an initial report, fill in the log up field with a dash.
- POC data shall be provided to include, at a minimum, the name, rank and position (i.e., CWO, LCPO, CSIO) of the individual submitting the report. Ensure a valid telephone number (if available) and e-mail address are included. For example: "POC/IT1 SMITH/CWO/ARLEIGH BURKE/PRIPHN:757-555-1212/EMAIL:SMITH4@DDG51.NAVY.MIL//"

The NCTAMS will include trouble ticket numbers in COMSPOT responses. These numbers will enable user commands to track incidents through the TMS. However, user commands will not be able to correlate trouble ticket numbers until the afloat interface for TMS is made available, which is currently planned for Increment II A, late 2008.

The following COMSPOT report will be used by all units:

Precedence - Up to IMMEDIATE is authorized

FM (Name of unit)

TO (Servicing NCTAMS)  
 (Servicing NCTS, if applicable)  
 (Communications Control Ship (CCS) if applicable)

INFO (Numbered Fleet Commander, if applicable)  
 (Strike Group Commander, if applicable)  
 COMNAVNETWARCOM NORFOLK VA (for all COMSPOT reports)  
 (Type Commander)  
 (Alternate NCTAMS)  
 (Other addressees as appropriate)

BT

CLASSIFICATION (As a minimum, should be CONFIDENTIAL)

MSGID/COMSPOT/(Originating Station PLA)/(Station Serial  
 Number/MON//

REF/(Appropriate Reference)/(Originators PLA)/(Date Time Group//

NARR/(Brief narrative describing the references)//

COMEV/(Type of issue)/(Start time)/(End time. Annotate with "-  
 " if ongoing)/(Type of service affected)/Trouble Ticket Number  
 Expressed as "Txxxxxx"//

LOCN/(Position expressed in longitude and latitude, or inport  
 location)//

RMKS/(Narrative of problem)

1. (U) This paragraph will contain the COMSPOT serial number, and indicate if it is an initial, updated, or final report.
2. (C) This paragraph will name the major system affected. For example, UHF SATCOM, Fleet SIPRnet Messaging, ADNS or INMARSAT.
3. (C) This paragraph will briefly describe the symptoms being observed. For example, "DOWN ON CWSP. UNABLE TO ACCESS NIPR, SIPR OR JCA SERVICES".
4. (C) This paragraph will describe actions taken by the originating station when a problem is discovered, or since the last submission. That can range from "ACKNOWLEDGE REF A", to "PERFORMED ERROR FREE BLACK BER WITH DISTANT END FOR 2 HOURS. COORDINATING RED BER."

5. (C) This paragraph will contain specific requests for support, actions, or services from the action addressees of the COMSPOT report.
6. (C) This paragraph will contain the ETR. It may read "UNKNOWN".
7. (C) This paragraph will contain the RFO. It may read "UNKNOWN" in an initial or update COMSPOT, but not in a final COMSPOT. In the event an RFO can not be determined for a final COMSPOT report, this paragraph will contain a synopsis of the actions taken in order to restore service.
8. (C) This paragraph is for narrative comments from the originator regarding this issue.
9. (C) This paragraph will contain POC information for the originating station. At a minimum, it will contain the name, rank and position of the individual submitting the report, i.e. "IT1 Smith, CWO". Also, include any and all e-mail addresses (NIPR and SIPR), telephone (commercial and DSN), or other method of direct contact.

DECL/(Declassification data)//

CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

**THIS PAGE INTENTIONALLY BLANK**



## APPENDIX C

### CONTENT INDICATOR CODES (CICs) FOR USE WITHIN THE USN

#### 1. USE OF CIC

The content indicator code (CIC) is used by the receiving communication terminal to determine distribution of data-formatted messages within AUTODIN. Annex B to ACP 128 describes and lists CICs for AUTODIN communications headers for DOD and inter-Service use. The structure of the CIC also allows each individual service to sub-allocate CICs for intra-service use.

Intra-Navy CIC assignments must coincide as much as possible with major/prime/minor categories listed in Annex B of ACP 128. When those blocks are exhausted, further assignments will be made using unassigned letters in the aforementioned categories.

#### 2. LIST OF USN CICs

The CICs listed below are the only codes authorized for intra-Navy use on messages sent in data format. However, the CIC "ZZEZ" may be used on data-formatted messages when none of these CICs are applicable.

<u>CODE</u>	<u>REPORT</u>
NBAA	High Value Asset Control (HIVAC) Transaction Reporting
NBAT	Ammunition Transaction and Stock Status Reporting
NBZA	Transaction Reporting
NCEA	Non-Combat Expenditure Allocations, and Interim and Tailored Allowance Data
NFBA	Fund Status Reporting Card Job Order/Fund Authorization Card
NFBC	Cycle Treasury Report
NFBE	Aircraft Cost Data
NFBF	Commitments and Obligations Cards
NFCB	Labor Job Time Card
NFCC	Attendance Time Card
NFCE	Personnel Action Reports

NFDC	Subsidiary Job Action
NFGD	Public Works Maintenance Cards
NFGE	Public Works Transportation Cards
NFLT	Financial Inventory Class 233
NGBA	Aircraft Engine Transaction Report
NGCC	Coast Guard Casualty Reporting System
NGCN	Casualty Reporting System (CASREPT)
NGGC	Navy Command and Control
NGHZ	Fleet Employment Schedule (FLTEMPSKD)
NGIZ	Operational Status Report/Force Status Report (OPSTAT/FORSTAT)
NGMA	XRAY Change Cards
NGMB	Flight Data Cards
NGMC	XRAY Locator Cards
NGMD	Not Operationally Ready Supply Aviation Item Reports (NORSAIR Hours)
NGZA	Navy Regional Data Automation Center (NARDAC)
NHAB	Military Standard Accounting Procedure (MILSTRIP) Transaction Cards
NHAC	Auxiliary Store Issue Cards
NHAE	Not Operationally Ready Supply Aviation Item Reports (NORSAIR)
NHAF	Consolidated Stock Status Reports (CSSR) Net Requirement Cards
NHAG	Auxiliary Store Planning Action Card
NHAH	Technical Control Card
NHAI	Auxiliary Store Material Transfer Card
NHAJ	Auxiliary Store Customer Requisition
NHAK	Inventory Tally Cards

NHAL	Optimum Consolidated Ships Allowance List (COSAL)
NHAM	Consolidated Ships Allowance List (COSAL) Area of Interest Decks
NHAO	Naval Oceanographic Office Transaction Reporting
NHBC	Logistics Management Interrogations
NHBD	Logistics Management Interrogation Replies
NHBE	Overhaul Work Stoppage Reports
NHBF	Navy Integrated Comprehensive Repairable Item Scheduling programs (NICRISP)
NHDE	Standard Navy Maintenance and Material Management System (SNMMMS)
NHDZ	Maintenance Data Systems
NHEF	Exchange of Engineering Data
NHHF	Change Notice Cards
NIAZ	Navy Ship Movements
NIBZ	Free World Merchant Shipping
NICZ	Bloc Merchant Shipping
NIDZ	Naval Control of Shipping/Military Sealift Command (NCS/MSC) Shipping
NISZ	Investigative Report
NJGB	COMSEC Material Transaction Reporting
NSTD	Exercise Table and Directory Change
NXCF	Exercise CASREP
NXEC	Exercise EMPSKD Changes
NXEG	Exercise EMPSKD Generation
NXNF	EXERCISE NAVFORSTAT
NZPO	Message containing non-literal information, pass to user with character integrity.

**THIS PAGE INTENTIONALLY BLANK**

## APPENDIX D

### C4I (COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS AND INTELLIGENCE) INFORMATION BULLETINS (CIBs) AND C4I ADVISORIES (CIAs)

#### 1. GENERAL

C4I Information Bulletins (CIBs) and Advisories (CIAs) are coordinated among each NCTAMS, Fleet CINC Communicator, Numbered Fleet Commander and appropriate Subject Matter experts to provide accurate, current reference and procedural information on a wide range of specific C4I subjects. CIBs are relatively permanent and are to be considered to have the force of directives; CIAs are relatively temporary and informative. CIBs and CIAs are promulgated by NCTAMS LANT through normal transmission channels and are posted at each NCTAMS SIPRNET homepage. Fleet units are required by their numbered fleet commanders to maintain a complete, current file of CIBs and CIAs for the use and guidance of operating personnel.

#### 2. CIB DESIGNATIONS

CIBs and CIAs are divided into Global, Joint and AOR-specific. Global CIBs/CIAs standardize procedures in all COMMAREAS, and the goal is to make all CIBs and CIAs Global whenever technically possible. Joint CIBs/CIAs standardize procedures in COMMAREAS and are controlled by the 2 NCTAMS. AOR-specific CIBs/CIAs apply to the COMMAREA controlled by a single NCTAMS and are labeled as LANT or PAC. In order to standardize CIB numbering Navy-wide, CIBs are divided into the categories listed in Global CIB 22A (Numbering of C4I information bulletins and advisories); these categories are further expanded by alphabetic characters (e.g., CIB 2A) to ensure all possible C4I subjects are included. The subject lines of CIBs and CIAs are preceded by the applicable COMMAREA to facilitate easy identification by fleet units using JMHS, AMHS, and Microsoft Outlook to read message traffic. CIAs are designated by sequential number and the year in which they are promulgated. For example, LANT CIA 03-01 denotes the third CIA of the year 2001 for the COMMAREAS controlled by NCTAMS LANT.

CIBs will be cancelled by date-time-group and by complete CIB designation. Global CIB 1 contains a complete listing of effective CIBs and CIAs; however, the SIPRNET homepage of each NCTAMS contain the definitive, most current listing.

#### 3. OBTAINING MISSING CIBS

CIBs and CIAs are GMF messages which cannot be obtained through service messages, (i.e., ZDK requests). Units not receiving CIBs and CIAs through normal transmission

distribution may obtain current copies by contacting the NCTAMS JFTOC by any means available or by going to the NCTAMS SIPRNET website. The SIPRNET homepage of each NCTAMS will maintain all effective CIBs and CIAs.

**APPENDIX E**  
**FREQUENCY EMISSIONS, BANDS AND DESIGNATIONS**

1. The DoD policy is that the term "hertz" will be the appropriate term for the unit of frequency to be used when referencing radio frequencies, frequency bands, or operating frequencies of communications-electronics equipment in all correspondence, records, standards, procedures, documents and, where applicable, on equipments.

REFERENCES.

DOD Directive 4650.1, Subject: Management and Use of the Radio Frequency Spectrum.

DOD Directive 5100.35, Subject: Military Communications-Electronics Board (MCEB).

DOD Directive 3222.3, Subject: DOD Electromagnetic Compatibility Program.

DOD JSC HDBK-80-11-1, Subject: Frequency Resource Record System (FRRS) Handbook, VOLUME I.

JCS MEMORANDUM MJCS 34-82, "Guidance on Joint and Inter-service Military Frequency Engineering and Management".

MCEB PUB 7, "Frequency Resource Record System (FRRS), Standard Frequency Action Format (SFAF)"

Naval Telecommunications Procedures (NTP) 6 Series, "Spectrum Management Manual".

2. FREQUENCY RANGE

Frequencies will normally be expressed as follows: In kilohertz (kHz) up to and including 29999 kHz., in megahertz (MHz) thereafter up to and including 3000 MHz., and in gigahertz (GHz) thereafter up to and including 3000 GHz.

The following internationally agreed designations may also be used:

<u>Frequency Sub-division</u>	<u>Frequency Range</u>
VLF (Very Low Frequency)	3 to 30 kHz
LF (Low Frequency)	30 to 300 kHz
MF (Medium Frequency)	300 to 3000 kHz
HF (High Frequency)	3000 to 30000 kHz

VHF (Very High Frequency)	30 to 300 MHz
UHF (Ultra High Frequency)	300 to 3000 MHz
SHF (Super High Frequency)	3 to 30 GHz
EHF (Extremely High Frequency)	30 to 300 GHz
(Not currently designated)	300 to 3000 GHz

### 3. NECESSARY BANDWIDTH (BW)

Express the necessary BW with exactly three numerals and one letter. The letter occupies the position of the decimal point and represents the unit of BW as follows:

1. H for Hertz
2. K for Kilohertz
3. M for Megahertz
4. G for Gigahertz

b. Fractional BW may be expressed to a maximum of two decimal places following the letter. The first character of the necessary BW shall always be greater than zero unless the necessary BW is less than 1 Hertz in which case the first character shall be the letter "H". Express the necessary BW as follows:!

(1) BW between .01 and 999.99 Hz shall be expressed in Hertz using the letter "H" in lieu of the decimal.  
Ex: 15H is 15 Hz of BW. 15H1 is 15.1 Hz of BW.

(2) BW between 1.00 and 999.99 KHz shall be expressed in Kilohertz using the letter "K" in lieu of the decimal.  
Ex: 2K is 2 KHZ of BW. 2K85 is 2.85 KHZ of BW.

(3) BW between 1.00 and 999.99 MHz of BW shall be expressed in Megahertz using the letter "M" in lieu of the decimal.  
Ex: 6M00 is 6 MHz of BW. 6M25 is 6.25 MHz of BW.

(4) BW between 1.00 and 999.99 GHz shall be expressed in Gigahertz using the letter "G" in lieu of the decimal.  
Ex: 10G00 is 10 GHz of BW. 10G25 is 10.25 GHz of BW.

### 4. DESIGNATION OF EMISSIONS

**EMISSION DESIGNATORS.** Listed below are the Table of Emission Classification Symbols and most common emission designators for equipment in the DOD inventory. If your equipment does not fit any of these emission designators call your respective Joint Frequency Management Office (JFMO) for assistance.



**Table E-1**  
**Required Emission Classification Symbols**

**First Symbol - Designates Type of Modulation of the Main Carrier**  
**Unmodulated**

N - Emission of unmodulated carrier

**Amplitude Modulated (AM):** An emission in which the main carrier is AM (including cases where sub-carriers are angle-modulated).

A - Double sideband

H - Single sideband, full carrier

R - Single sideband, reduced or variable level carrier

J - Single sideband, suppressed carrier

B - Independent sidebands

C - Vestigial sidebands

**Angle-Modulated:** An emission in which the main carrier is angle-modulated.

F - Frequency modulation (FM)

G - Phase modulation

**Amplitude and Angle-Modulated:** Emission in which the main carrier is amplitude modulated and angle-modulated either simultaneously or in a pre-established sequence pulse. (See Note)

D - Main carrier is amplitude-modulated and angle-modulated simultaneously or in a pre-established sequence

**NOTE:** Emission, where the main carrier is directly modulated by a signal which has been coded into quantized form (pulse code modulation (PCM)), shall be designated as either an emission in which the main carrier is AM, or an emission in which the main carrier is angle-modulated.

**Pulse**

P - Sequence of unmodulated pulses

K - Modulated in amplitude

L - Modulated in width/duration

M - Modulated in position phase

Q - Carrier is angle-modulated during the period of the pulse

V - Combination of the foregoing or is produced by other means

**Combination**

W - Cases not covered above in which an emission consists of the main carrier being modulated, either simultaneously or in a pre-established sequence, in a combination of two or more of the following modes: amplitude, angle, pulse

**Other**

X - Cases not otherwise covered

**Second Symbol - Designates the Nature of Signal(s) Modulating the Main Carrier**

0 - No modulating signal

1 - A single channel containing quantized or digital information without the use of a modulating sub-carrier. (Excludes time-division multiplex (TDM))

2 - A single channel containing quantized or digital

information, using a modulating sub-carrier  
3 - A single channel containing analogue information  
7 - Two or more channels containing quantized or digital information  
8 - Two or more channels containing analogue information  
9 - Composite system with one or more channels containing quantized or digital information, together with one or more channels containing analogue information  
X - Cases not otherwise covered

**Third Symbol - Type of Information to be Transmitted**

N - No information transmitted  
A - Telegraphy - for aural reception  
B - Telegraphy - for automatic reception  
C - Facsimile  
D - Data transmission, telemetry, telecommand  
E - Telephony (including sound broadcasting)  
F - Television (video)  
W- Combination of the above  
X - Cases not otherwise covered

**Optional Emission Classification Symbols**

**Fourth Symbol - Designates the Details of Signal(s)**

A - Two-condition code with elements of differing numbers and/or durations  
B - Two-condition code with elements of the same number and duration without error correction  
C - Two-condition code with elements of the same number and duration with error correction  
D - Four-condition code in which each condition represents a signal element of one or more bits  
E - Multi-condition code in which each condition represents a signal element of one or more bits  
F - Multi-condition code in which each condition or combination of conditions represents a character  
G - Sound of broadcasting quality (monophonic)  
H - Sound of broadcasting quality (stereophonic or quadraphonic)  
J - Sound of commercial quality (excluding categories defined for symbol K and L below)  
K - Sound of commercial quality with the use of frequency inversion or band splitting  
L - Sound of commercial quality with separate frequency modulated signals to control the level of demodulated signal  
M - Monochrome  
N - Color  
W - Combination of the above  
X - Cases not otherwise covered

**Fifth Symbol - Designates the Nature of Multiplexing**

N - None  
C - Code-division multiplex (includes bandwidth expansion techniques)  
F - Frequency-division multiplex  
T - Time-division multiplex  
W - Combination of frequency-division multiplex and time-

division multiplex  
X - Other types of multiplexing

### **Most Common Emission Designators**

#### **HF (2-30 MHz)**

Carrierwave (CW)	100HA1A
Single channel single sideband (SSB) voice, suppressed carrier	3K00J3E
Single channel teletype (TTY)	1K10F1B
Multi-channel independent sideband (ISB)	6K00B7B
2 sidebands both TTY Multi-channel independent sideband (ISB),	6K00B8E
2 sidebands both voice Multi-channel independent sideband (ISB),	6K00B9W
2 sidebands combined voice/TTY Independent Sideband (ISB), 2 sidebands, combination voice/data	9K00B9W

#### **VHF/FM (30-88 MHz)**

Single channel digital data	25K0F2D
Single channel analog data	25K0F3D
Single channel digital voice	25K0F2E
Single channel analog voice	25K0F3E
Single channel (FM) voice	30K0F3E
Single channel voice (secure)	32K0F1E or 37K5F1E
Single channel data	32K0F1D or 37K5F1D

#### **VHF/FM (138-174 MHz)**

Single channel voice	8K50F3E or 16K0F3E
Single channel voice (PRC127)	12K0F3E
Single channel voice (DES)	8K50F1E or 20K0F1E

**VHF/AM (118-137 MHz)**

Single channel, double-sideband, AM voice 6K00A3E

**UHF/FM (420-470 MHz)**

Single channel voice 8K50F3E or  
16K0F3E

Single channel voice (DES) 8K50F1E or  
20K0F1E

Single channel (FM) voice/data 1M30F9W

Pulse modulated without modulating signal or information  
transmitted 2M00P0N

**UHF/AM (225-400 MHz)**

Single channel voice 6K00A3E

Single channel voice (secure) 25K0A1E or  
37K5A1E

For applicable use of Frequency Emissions and Designators  
refer to NTP 6, Annex A.

## APPENDIX F

## MILITARY AFFILIATE RADIO SYSTEM (MARS) OPERATIONS

## REFERENCES:

- a. NTP 8
- b. MARS Area Operations Guides

1. PURPOSE. To provide information on Military Affiliate Radio System (MARS) operations.

2. GENERAL

It is the policy of the Department of the Navy to support MARS. Basic policy instructions and guidance for MARS operations within Navy and Marine Corps activities are contained in references (a) and (b).

The primary purpose of the MARS program is for EMERGENCY/AUXILIARY communications among military, civil and disaster officials.

A secondary function is to assist in effecting normal Naval communications under emergency conditions and the handling of morale and quasi-official communications for US Government personnel throughout the world.

There are MARS communication areas: Northeast, Central, South, and Pacific. Each area has their own operations guide which is used as a supplement to reference a. These guides can be found on the MARS website, <http://www.navymars.org>.

3. PROCEDURES

MARS operations afloat are authorized throughout LANTFLT/ PACFLT underway and inport under normal, routine peacetime conditions, unless:

- a. Operational chain of command interposes objections.
- b. EMCON is imposed.
- c. Foreign port host government regulations do not permit operations.
- d. Assigned sensitive, highly classified movements.

An afloat MARS station is considered a "station under military auspices" and, therefore, does not require a licensed amateur radio operator. However, use of personnel with amateur radio experience is highly recommended.

Ships desiring to operate as MARS stations are exempt from the

application procedures prescribed in references (a) and (b) but shall apply as follows:

- Submit a message request using the current GENADMIN format such as:

```

ROUTINE DTG
FM REQUESTING UNIT
TO CHNAVMARCORMARS WILLIAMSBURG VA
   APPROPRIATE FLEET CDR
INFO (NUMBERED FLEET COMMANDER WHEN UNDER THEIR OPCON/TACON)
   (TYPE COMMANDER)
   (OPERATIONAL COMMANDER)
BT
UNCLAS //N02090//
MSGID/GENADMIN/ORIGINATOR'S PLA//
SUBJ/MARS AFLOAT OPERATION//
POC/NAME/CODE/DSNPHONE/CMLPHONE//
RMKS/1. UNODIR INTEND CONDUCT MARS OPS FM----- TO----- .
2.COMMAND MARS OFFICER OR STATION CUSTODIAN: NAME, SSN,
RANK, SVC, LICENSE NUMBER/MARS CALL SIGN/EXP DATE (IF APPLICABLE)
3.COMMAND MARS CHIEF OPR OR AUTHORIZED OPR: NAME, SSN,
RANK, SVC, LICENSE NUMBER/MARS CALL SIGN/EXP DATE (IF APPLICABLE)
4.UNITS CURRENT MAILING ADDRESS. //
BT

```

- Operational/type commanders objecting to MARS Afloat operation shall inform COMLANTFLT or COMPACFLT, CHNAVMARCORMARS to preclude inadvertent licensing of an afloat unit.
- If no objection to the request is interposed by the chain of command within ten working days, CHNAVMARCORMARS WILLIAMSBURG VA will reply with an official message assigning the MARS call sign and will mail station license, a copy of Pacific/Atlantic Afloat Specialty Network current operations guide and other pertinent information.

Frequencies will be assigned IAW NTP 8 or by CHNAVMARCORMARS and will comprise the Pacific or Atlantic MARS Afloat Specialty network, respectively.

MARS is a non-secure system. The responsibility for maintenance of proper standards of security by personnel using shipboard MARS radio facilities rests with the commanding officer. The commanding officer shall:

- a) Promulgate detailed instructions on control and operation of MARS. Security education programs should include procedures to prevent inadvertent disclosure of classified information when using MARS.

- b) Ensure that conversations are limited to unofficial, unclassified personal topics. Phone patches to detailers from afloat units are authorized. Any message, which may result in financial or material gain, is considered business in nature and will not be handled via MARS.
- c) Designate an officer as Command MARS Officer with responsibility to the commanding officer for control and security of the MARS station.
- d) Designate an operator as Command MARS Chief Operator with responsibility to the Command MARS Officer for control and operations of the MARS station.

Operational commanders shall provide direction for control of MARS operations as part of EMCON instructions.

The Numbered Fleet Commanders and Type Commanders will review reports of security violations, take corrective action as necessary, and, if warranted, suspend or cancel MARS radio operations in the unit concerned.

Commanding officers and Command MARS Officers shall be familiar with the regulations and instructions relative to operating stations in foreign ports and third party communications.

COMSEC monitoring of MARS will periodically occur. The purpose of COMSEC monitoring of MARS is to ascertain and reduce security vulnerabilities. In order to satisfy DOD requirements concerning the consensual monitoring of MARS communications for COMSEC purposes, the following actions shall be accomplished at each command having a MARS station:

1. Retain on file for a period of one year a consent form signed by prospective MARS users which states: "I understand that periodic COMSEC monitoring of MARS conversations will occur and use of MARS equipment constitutes consent to such monitoring."
2. Before a telephonically originated call is connected, the MARS operator will:
  - a. Ensure the caller has a current consent form on file.
  - b. Orally advise the caller that MARS communications are subject to monitoring. After the caller acknowledges this statement, a log entry will be made and the call completed.
3. A sign stating, "MARS COMMUNICATIONS ARE SUBJECT TO COMMUNICATIONS SECURITY MONITORING AT ALL TIMES. USE OF MARS CONSTITUTES CONSENT TO COMMUNICATIONS SECURITY MONITORING" shall be displayed in full view of MARS users.

4. In cases of emergency in which the call must be placed immediately and no consent form is on file, the following procedures will apply:

- a. Orally advise the caller "MARS communications are subject to periodic COMSEC monitoring and use of MARS constitutes consent to monitoring."
- b. After the caller acknowledges this statement, a log entry will be made and the call completed. The log entry shall note the nature of the emergency, oral notification, and acknowledgement by the caller.



## APPENDIX G

### VISUAL COMMUNICATIONS

#### **Description and Purpose**

Visual signaling is a means of passing tactical and administrative information between ships within visual signaling range, and between ships and signal stations ashore. Methods employed are flashing light (directional and non-directional, including infrared), flag hoist, semaphore, colored lights, and pyrotechnics. Quartermasters also perform submarine, ship, and aircraft recognition and identification, communications with non-allied naval and merchant ships, and special signaling during amphibious operations, convoy escort, and underway replenishments.

The U.S. Navy reserves several signals for its own use, such as those contained in the USN ADDENDUM to ATP 1 VOL II (when in force), and the U.S. SUPPLEMENT to ACP 131. This chapter covers areas not specifically addressed in allied publications and amplifies existing instructions where needed. When operating exclusively with units of the U.S. Navy, the procedures prescribed herein shall govern.

#### **Security**

All personnel whose duties require them to handle classified material must be familiar with SECNAVINST 5510.36 series (Department of the Navy Information and Personnel Security Program). Signal bridge personnel must possess the security clearance commensurate with the material handled. A training program, stressing the importance of safeguarding classified material, must be kept in force at all times. The signal watch must diligently protect classified material. Quartermasters must be trained in communications security (COMSEC) by becoming familiar with Chapter 4 of this publication and EKMS-1 (series).

Signal bridge personnel also have the responsibility of storage and care for equipment that is susceptible to pilferage. The loss of equipment such as binoculars, night observation devices, flares and multipurpose lights is not only costly, but can seriously hamper the mission of the signal bridge and jeopardize the safety of the ship.

#### **Publications**

In addition to the publications that are customarily kept on the signal bridge, Quartermasters must be aware of other publications that are maintained onboard. The ship's naval warfare publications librarian maintains an index of these publications

as well as information on allowances and procurement.

Because communications requirements change constantly, governing documents are subject to frequent updates and changes should be entered immediately unless otherwise stated. See paragraph 1.5.5 of this publication for complete information on communications publications and changes.

Changes or corrections to PUB 102, International Code of Signals, are normally issued through Notice to Mariners (N/M) messages. The Navigation department maintains the correction card for PUB 102.

In addition to publications, there are many notices and instructions issued by various commands that are of interest to visual communications personnel. OPNAV NOTE 5215 (Consolidated Subject Index), distributed semi-annually, contains a complete list of instructions issued by Washington headquarters organizations. The ship's administrative office normally maintains these notices and instructions.

### **Operation Orders**

Prior to beginning an underway period, all signal bridge personnel must be familiar with the communications portion of the operation order (OPORD) or letter of instruction (LOI). The Leading Quartermaster should obtain the OPORD or LOI from the communications officer. The Leading Quartermaster must consult the OPORD frequently to insure the signal team is kept up-to-date on any changes

At a minimum, the signal bridge must have a list showing the Task Organization, call signs, schedule of events and any special lighting measures or signals. The Leading Quartermaster of ships assigned to the Task Organization will meet for a pre-underway brief to cover visual communications, use of call signs, drills, etc. A great advantage will be gained by discussing these items prior to sailing. The staff or leading Quartermaster of the senior ship will initiate such meetings.

### **Standard Operating Procedures (SOPs)**

The Leading Quartermaster must maintain a set of SOPs and/or standing orders on the signal bridge with a provision for each individual's signature indicating their familiarity with such orders. These SOPs shall be reviewed and signed at the discretion of the leading Quartermaster. The leading Quartermaster usually drafts these orders and the communications officer or Navigator reviews and approves them. They contain guidelines tailored to the unique requirements of a signal bridge, e.g., traffic handling and message routing, duties and

conduct of watch standers, publication/equipment/log accountability, and certification of personal signs, safety precautions, and visual message release authority.

### **Training**

Maintain a separate log for the purpose of recording visual communications drills and exercises. Keep the format the same as that of the official log, but label the drill log clearly as such. Destroy the drill log by the same method as that prescribed for the official log. There is no retention requirement for the drill log after the final entry.

In conjunction with the drill log, maintain a separate visual station file for visual communications drill messages. Label, maintain, and destroy this file consistent with the instructions for the drill log. There is no retention requirement for the drill visual station file.

Quartermasters must contend with poor visibility, heavy seas, changing tactical formations and other adverse conditions. All these serve to hinder operators and place a unique burden upon the communications effort. Quartermasters will not be able to effectively contribute to the mission of the signal bridge if not thoroughly qualified. Therefore:

(1) Every effort will be made to conduct visual communications training between ships while in company. When steaming independently, quartermasters shall conduct daily training amongst themselves. Visual training shall be a part of the daily routine when possible;

(2) Leading Quartermasters onboard flagships shall coordinate visual training between ships within the strike group and schedule periodic meetings to discuss problem areas and future training schedules.

### **Performance Testing**

The Personnel Advancement Requirements (PAR'S) stipulate that personnel in the QM rate must successfully complete flashing light and semaphore performance tests prior to recommendation for advancement. Appendix E of the Navy Enlisted Manpower and Personnel Classifications and Occupational Standards (NAVPERS 18068F) contains a list of the required performance tests. Performance tests may be ordered per provisions contained in the Advancement Manual, (BUPERSINST 1430.16), or prepared locally using the following criteria:

(1) Each coded message text must include all letters of the alphabet, numerals 0 through 9, and all punctuation symbols listed in ACP 130. Do not include the word drill in text;

(2) Each plain language message text shall contain subject matter consistent with that of an official naval message, but shall not include the security classification, the word drill or phonetic spelling. Punctuation symbols shall be used in semaphore messages;

(3) To determine the required number of words in the plain language text, count each letter, numeral and punctuation symbol as one character. Five characters are equivalent to one word. The text of flashing light and semaphore messages will contain the required number of words or coded groups, and shall be sent and received at a minimum of three words per minute.

A qualified observer must be present during performance testing. An observer shall be senior in pay grade to individual being tested. No individual will be administered a performance test for a pay grade which is more than one pay grade above that currently held. Recommend using an assist ship to administer performance tests. Responsibility for observer selection lies with the Communications Officer, and shall be in the following order:

- (1) QM assigned by Staff;
- (2) Senior QM of assist ship;
- (3) Senior QM from any other ship;
- (4) Senior QM onboard.

Duties of performance test observer:

- (1) Provide performance test messages and safeguard against compromise prior to test;
- (2) timing test message:
  - (a) Use stopwatch or similar timing device;
  - (b) Time message text only. Allow three words per minute for flashing light and semaphore messages. Messages transmitted must not differ from those received by an individual;
  - (c) Allow one error in each plain language message transmitted/received by flashing light;
  - (d) Allow two errors in each semaphore message transmitted/received; however, only one error may be charged to any one word.
  - (e) Allow two errors in each coded message transmitted/received by flashing light.
- (3) Submit performance test results to individual via leading Quartermaster and Communications Officer.

Upon satisfactory completion of performance testing, leading Quartermaster must ensure service record entry is recorded per instructions contained in Chapter 7 of the Advancement Manual, (BUPERSINST 1430.16)

Personnel who were given a performance test waiver to advance to next higher pay grade must be given applicable performance tests within sixty days after returning to Quartermaster duties. Appropriate service record entry must be made upon satisfactory completion of tests.

### **Supervisors**

The Leading Quartermaster is responsible for the overall efficient operation of the signal bridge. This in no way diminishes the responsibility of watch supervisors to exercise the initiative and foresight necessary to maintain a top signal team.

Signal watch supervisors are to ensure:

(1) Smooth flow of information between the ship's bridge, the signal bridge and the combat information center. Close monitoring of information passed over Interior Communications (IC) circuits is essential. Call signs and substitutes must be broken prior to passing over these circuits;

(2) Quartermaster of the watch standers will work with ships lookouts to bring a call-up or flag hoist signal to their attention. Visual communications are the responsibility of all bridge watch personnel;

(3) Appropriate recommendations are passed down to the bridge team and flag bridge when a flag officer is embarked with his staff;

(4) Visual communications training is conducted during every watch when possible;

(5) Watch standers comply with ACP 130, article 102.

### **Unofficial Signaling**

Unofficial operator-to-operator traffic signaling during watches is an effective means of maintaining and increasing operator efficiency. The Leading Quartermaster should encourage training during watches on a not to interfere with normal operations basis. Although there is normally no objection to such signaling in peacetime, obtain permission to do so from the OOD. Personnel engaged in unofficial signaling must always be alert to the danger of inadvertently revealing classified information regarding past or future ship movements, exercises, casualties,

etc.

Unofficial signaling between ships and private individuals ashore is prohibited.

### **Signaling Ships of The Former Soviet Union**

On 25 May 1972, the governments of the U.S. and the U.S.S.R. signed an agreement containing procedures designed to prevent incidents on and over the high seas. This is called the INCSEA Agreement and is promulgated within the U.S. Navy as OPNAVINST C5711.96. As part of the agreement a special table of signals was drafted for use between United States and Soviet warships and auxiliary vessels. The INCSEA agreement now extends to the former Soviet Union (see Notice to Mariners 18/92).

Signal personnel should pay particular attention to the requirement to hoist "YVp1" which indicates signals from the INCSEA Agreement, and "YVp1 TACK ZLp1" which answers/acknowledges signals from the INCSEA Agreement. Do not hoist the answer/acknowledgement signal at the dip. Instead, hoist it close up after receiving permission from the Commanding Officer via the OOD.

### **Signaling Merchant Ships**

When signaling merchant ships use flashing light as the primary visual method. Merchant ships use flag hoist to a limited degree and semaphore use is not a requirement. Bridge-to-Bridge radiotelephone has resulted in a further decrease in visual communications use by merchant ships and often, after visual communications have been established, the merchant will request a shift to radiotelephone, or will sometimes respond to a visual call by radiotelephone. Signal personnel must be thoroughly familiar with Chapter 1, Sections 8 and 10 of PUB 102, International Code of Signals, and bridge-to-bridge radiotelephone regulations contained in COMDTINST M16672.2, Navigation Rules, International - Inland.

As with all signaling, conduct communications with merchant ships in a courteous and professional manner.

Unless higher authority directs otherwise, determining the identity/nationality of merchant ships by exchanging international call signs is authorized. U.S. Naval vessels may identify status by flashing "DE US NAVY" or "DE US MAN OF WAR".

### **Communicating With Aircraft**

When Signaling between aircraft and surface vessels is normally conducted only during aircraft emergencies and is slow and difficult at best. In the event signaling with aircraft is required, the ship's signal team must be alert to interpret intelligence conveyed by aircraft maneuvers. Surface vessels

should establish the identity of an aircraft prior to any effort to communicate by flashing light. Due to the speed of the aircraft use a multi-purpose light to achieve the most efficient communications.

Because communicating with aircraft is slow and difficult, the Leading Quartermaster will ensure frequent exercises are conducted to improve skills in this area.

Chapter 6, Section 6 of ATP 1 VOL I contains aircraft emergency signals. Extracts are permitted and must be readily available on the signal bridge.

PUB 102 (International Code of Signals), Chapter 4, Section 2 contains international signals used by aircraft engaged in search and rescue operations.

### Call Signs

Single letter type indicators for U.S. Naval ships and craft are derived from SECNAVINST 5030.1 (Classification of Naval Ships and Craft) are reflected below:

"A"	AUXILIARIES/ LOGISTICS	ACS AD AE AFS AG AGF AGM AGOR AGOS AGS AGSS AH AK AKR AO AOE AOR AOT AP ARC ARS AS ATF AVB
"B"	BATTLESHIPS	BB
"C"	CRUISERS	CG CGN
"D"	DESTROYERS	DD DDG
"F"	FRIGATES	FF FFG
"L"	AMPHIBIOUS/ ASSAULT	LCAC LCC LCM LCPL LCU LHA LHD LPD LPH LSD LST LSV SDV
"M"	MINE WARFARE	MCM MHC
"N"	MINE CONTROL SHIP	MCS
"P"	PATROL	ATC PB PBR PC(R) PCF PG PHM(R)
"R"	AIRCRAFT CARRIERS	CV CVN
"S"	SUBMARINES	SSBN SSN
"Y"	SUPPORT CRAFT	AFDL AFDM ARD ARDM DSRV DSV IX TR YDT YPD YFU YO YOG YP YTB YTT

**U.S Naval Ships and Crafts Type Indicators**

The Intra-USN type indicator "U" is used to denote "SURFACE" organizations established by COMNAVSURFLANT/COMNAVSURFPAC and precedes or follows Group/Squad/Div to construct collective or commander call signs:

U DIV	THIS SURFACE DIVISION
U GROUP p4	SURFACE GROUP FOUR
SQUAD U	COMMANDER THIS SURFACE SQUADRON

**Intra-USN type indicators**

Unless otherwise directed by local authorities, ships entering or leaving port during daylight hours (sunrise to sunset) shall display their international call sign from the most inboard port halyard. The address group of embarked flag officers or unit commanders, when embarked, shall be displayed from the most inboard starboard halyard. There are instances when an embarked flag officer eligible for command at sea is not assigned an address group. The personal flag of such a flag officer shall nonetheless be flown per Chapter 12, Navy Regulations. Outboard halyards must remain free for emergency or tactical signals.

Ships entering or leaving United States ports normally hoist/haul down their call sign and address group when crossing the boundary of international-inland water (line of demarcation). However, the port and vessel traffic geographical configuration must also be considered. Ships entering foreign ports must consult appropriate sailing directions for any local regulations regarding the display of call signs.

In addition to the call sign/address group, ships entering port will display the Designation (DESIG) pennant followed by berth assignment when U.S. or Allied Naval authorities are present.

Ships underway for the purpose of shifting berths within the boundaries of a U.S. Naval base will display the DESIG pennant followed by berth assignment in lieu of call sign/address group.

Ships entering port at night where U.S. or Allied Naval authorities are located may identify themselves by transmitting on yardarm blinkers the prosign "DE," the flag call (if embarked), followed by a slant and the international call sign. (EX: DE JZCP/NSBR.) Berth assignment may also be transmitted in this manner preceded by DESIG or appropriate operating signal.

When it is known that Military Sealift Command (MSC) ship has a military detachment with Quartermaster embarked, it may be called by its visual call sign. Otherwise use the international call sign.



The use of special Task Organization call signs contained in ACP 130 is extended to intra-USN messages transmitted by flashing light. The following are examples of this type of call sign and transmission by all methods:

<u>COMMANDER CALL</u>	<u>FLAGHOIST</u>	FLASHING LIGHT	FLASHING LIGHT/ <u>SEMAPHORE (intra-USN)</u>
CTF 50	0p5p0	CTF 50	ZERO p5p0
CTG 50.3	*1p3	CTG 50.3	*ONE p3
CTU 50.3.5	*2p5	CTU 50.3.5	*TWO p5
CTE 50.3.5.1	*3p1	CTE 50.3.5.1	*THREE p1
COMSIXTHFLT	4p6	COMSIXTHFLT	FOUR p6

COLLECTIVE CALL

TF 50	6p5p0	TF 50	SIX p5p0
TG 50.3	*7p3	TG 50.3	*SEVEN p3
TU 50.3.5	*8p5	TU 50.3.5	*EIGHT p5
TE 50.3.5.1	*9p1	TE 50.3.5.1	*NINE p1

- Denotes within own Task Organization

**NOTE:** A Task Force is subdivided into groups, units, and elements at the discretion of the Task Force commander. The particular group, unit, or element to which a fleet/mobile unit is assigned is contained in the OPORD, along with mission and subordinate commanders.

Because Daily Changing Call Signs (DCCS) for Task Organizations are designed primarily for radio communications, their use may be extended to visual communications only if security of the address is required.

For intra-USN use, the visual call sign "P9P9" may be used to call, address, indicate or denote the Officer Conducting Exercise (OCE).

In situations where ships with identical visual call/shortened visual calls, e.g., LP1P0, are operating in the same Task Organization, the Task Commander may specify in the OPORDER the use of a special visual call sign to avoid confusion within his/her own Task Organization. If not specified in OPORD refer to ACP-130, article 210a.

**Examples:** LPH-10...LP0  
LPD-10...LP1P0

These call signs may be used for calling, answering, relaying and in the address of visual messages delivered solely by visual means. This does not preclude the use of command calls where appropriate.

### **Methods of Transmission**

Directional flashing light is a means of passing traffic to a single unit using visible or infrared light. This method uses a 12-inch searchlight or a small multi-purpose (portable) light. During hours of darkness the 12-inch signal searchlight and multi-purpose light are fitted with:

- (1) Amber filter for normal steaming (aircraft carriers are authorized to use blue filter);
- (2) Red filter for flight operations and replenishments;
- (3) Red filter with reducing diaphragm when maneuvering alongside;
- (4) Infrared hood on 12-inch signal searchlight when required.

Non-directional flashing light enables simultaneous transmission to more than one unit and uses white yardarm blinker lights or infrared beacons. Both are used during hours of darkness and provide 360 degree coverage. OOD and OTC permission must be granted prior to using white yardarm blinker lights due to brilliancy.

Flag hoist is a non-directional means of transmitting signals with predetermined meanings taken from authorized publications. The U.S. and Allied navies use 68 different flags/pennants or combinations thereof for this purpose.

Semaphore may be considered directional or non-directional; however, non-directional procedures are used during transmission. This method uses small hand flags during daylight hours and wands fitted with red lenses during hours of darkness. Signal personnel must take care to avoid confusion with paddle/wand signals from replenishment stations while conducting alongside operations.

Additional non-directional methods for transmitting signals with predetermined meanings are:

1. Pyrotechnic signaling using rockets, flares, or colored smoke;
2. Day shapes
3. Colored lights, either fixed or flashing

### **Infrared Signaling**

Infrared signaling is normally ordered during periods of darken ship, but may be used at any time visible light systems are considered inappropriate. Ships with traffic for transmission

may notify addressees by secure voice radio using the code word "NANCY HANKS," or the relevant signal from ATP 1 VOL II or ACP 131. Depending on the degree of darken ship in effect, addressees may also be notified by flashing light using the code word "NANCY." Additionally, the OTC may establish infrared calling periods eliminating the need for an operator to continuously monitor an infrared receiver.

Point of Train Lights (POT) remain on during transmission when communicating with directional infrared searchlights using "directional flashing light procedure". They are turned off at all other times.

### **Flag Hoist Procedures**

This paragraph amplifies flag hoist procedures prescribed in ACP 130 and also explains unique intra-USN requirements.

When an addressee desires to question a signal, the signal shall be hoisted at the dip and the INTERROGATIVE pennant hoisted close-up on an adjacent halyard. The call sign of the originator does not need to be hoisted when in direct communication.

1. The originator must acknowledge an INTERROGATIVE signal, unless such signal can be clarified or canceled immediately.
2. The INTERROGATIVE pennant may be amplified and used as indicated below. These signals are most effective in expediting flag hoist signals when passed by flashing light. Once operators identify the problem they should adhere to the procedures in ACP 130 for canceling or correcting a hoist to avoid the possibility of early execution or further delay of communications.

### **SIGNAL**

### **MEANING**

INT(CHAPTER GROUP)

This signal not understood. Used when questioning one signal if multiple signals are flying). Should the hoists consist of two or more signals from the same chapter group, use basic group, but in either case to maintain brevity, suffixes need not be transmitted.

INT 1

Signal now flying not distinguishable;



SHIP TO BOAT FLASHING LIGHT "TAPS CODE"		
MEANING	SHIP	BOAT
Steer straight <u>away</u> from ship	Flash series of "A"s	Answer with series of "A"s
Steer straight <u>toward</u> ship	Flash series of "T"s	Answer with series of "T"s
Standby for <u>port</u> turn	Flash series of "P"s	Answer with series of "P"s
Commence slow port turn	Steady light	Steady light
Stop turn, steady on present course	Drop steady	Drop steady
Standby for <u>stbd</u> turn	Flash series of "S"s	Answer with series of "S"s
Commence slow stbd turn	Steady light	Steady light
Stop turn, steady on present course	Drop steady	Drop steady
Return to ship	Flash series of "Q"s	Answer with series of "Q"s
BOAT TO SHIP FLASHING LIGHT "ARC CODE"		
MEANING	BOAT	SHIP
Need <u>assistance</u>	Flash series of "A"s	Flash "RRR"
Have <u>recovered</u> man	Flash series of "R"s	Flash "RRR"
<u>Cannot</u> find man	Flash series of "C"s	Flash "RRR"

**BOAT SIGNALS**

BOAT SIGNALS (SHIP TO BOAT)		
FLAGHOIST	PYROTECHNICS	MEANING
SEE ATP 1, VOL II	ONE WHITE STAR	Steer straight away from ship
	ONE RED STAR	Steer left (to port)
	ONE GREEN STAR	Steer right (to starboard)
	TWO GREEN STARS	Steer straight toward ship
	TWO WHITE STARS	Steady on present course
	TWO RED STARS	Return to ship

BOAT SIGNALS (BOAT TO SHIP)	
PYROTECHNICS	MEANING
ONE GREEN STAR	Cannot find man
ONE WHITE STAR	Have recovered man
ONE RED STAR	Need assistance

PREP shall be used to observe sunrise.

FLAG	INDICATOR	NORMALLY DISPLAYED	MEANING
PREP	SUNRISE	AT YARDARM. REPEATED BY ADDRESSEE(S) (NOT UNDERWAY)	CLOSE UP: 5 MINUTE STANDBY  HAULED DOWN: OBSERVE SUNRISE

**Use of Prep for Sunrise**

Emergency alarm signals are to be repeated by all ships, with the call sign of the originator, if other than the OTC, below 1st SUB hoisted close-up on adjacent inboard halyard. Reference ATP-1(C) VOL. II, Article 300(B) and Article 302.

Speed flags should be used when entering or leaving port only if U.S. or allied naval units are also underway in the vicinity. Speed flags are of no interest to ships pier side or at anchor, nor do they carry any meaning to non-allied naval ships or merchant ships.

The senior officer among a nest or group of ships will assign a visual communications duty ship for the nest/group. This ship will display the visual guard flag during daylight hours, and will transmit, answer, receipt for and deliver all visual traffic for the nest/group. In addition, this ship will display the prep flag for sunrise, morning and evening colors for all ships in the nest/group. The use of prosigns to indicate relay/transmission to other ships in the nest/group is not required.

### **Double Flash Procedure**

This procedure, explained in ACP 130, article 607, is used when no recorder is available and removes the element of speed from a visual transmission. Since the ship's bridge area is continuously manned while underway, operators shall use prudence and good judgment before asking for double flash procedure.

### **Signal Handling**

All signals transmitted by flag hoist, flashing light, or semaphore are tactical, informative, or administrative in nature. Visual communications use the following signal publications most frequently:

1. ATP 1 VOL II (Allied Maritime Tactical Signal and Maneuvering Book);
2. ATP 2 VOL II (Allied Naval Control of Shipping Manual Guide to Masters);
3. ACP 131 (Operating Signals);
4. NWP 22-3 (Ship-to-Shore Movement);
5. PUB 102 (International Code of Signals).

Unless instructions indicate otherwise, a signal may be sent using any authorized visual transmission medium; however, the method of transmission has no bearing on the action to be taken upon receipt of the signal. All signals must be handled promptly.

The intra-USN message format using signals from ATP 1 VOL II will not contain a DTG/TG in the heading/ending.

### **Visual Messages**

When a message has been released for visual transmission but no specific method is identified, the signal watch supervisor will

select the most appropriate method for passing the message.

The following provides recording information for the visual message form:

1. CALL UP BLOCK. Show all contents of the call element exactly as transmitted/received; (See ACP 130, article 116.)
2. DATE BLOCK. Show Local date;
3. SYSTEM BLOCK. Show method of transmission used. For outgoing message, show method used for final TOD;
4. TOR/TOD BLOCK. Circle whichever applies, and enter time of receipt or time of final delivery using GMT;
5. OPERATOR and SUPERVISOR BLOCK. Each must insert own personal sign which is used for servicing and endorsing station records and messages. No two individuals are to use the same personal signs within a watch station. Care must be taken to insure that a personal sign does not conflict with a prosign, operating signal or abbreviation used to denote methods of transmission. Personal signs shall be the same as those certified in the signal bridge standing orders or standard operating procedures (SOP);
6. DTG BLOCK. Show DTG MO YR or TG/DATE MO YR as applicable. The assignment of a DTG to an outgoing visual message will be coordinated with the telecommunications facility to avoid duplication;
7. FROM/TO/INFO/XMT BLOCKS: Show plain language breakdown of call signs. "USS/USNS" and hull designator are optional. Corresponding designators for foreign ships must be used;
8. Show separate signs as transmitted/received.
9. The service cross (shown below) may be placed on front or back of the message form. If on back, enter "OVER" in DTG BLOCK to right of year.

Deliver a copy of all outgoing and incoming visual messages, except signals, to the telecommunications facility for inclusion in the master files. Telecommunications facility personnel will endorse unclassified originals and return them to the signal supervisor for filing in the visual station file. For classified messages, the original will be retained in the classified portion of the telecommunications facility files and a filler endorsed by telecommunications facility personnel, will be placed in the visual station file.



TRAINING MESSAGE  
 OPNAV FORM 8110-20 (10-88)  
 Reorder from 77543 Com. T. HSCA (NAPA) S/N 0107-708-8 000

CALL UP Fp8 DE Rp7

READING T ZWL p2A P 032300Z JAN 95 FM 1p3 TO 7p3  
 GR7 BT

LNCLAS	THIS	MESSAGE	FOR	SAMPLE	
USE	ONLY.	BT	K		5
					10
					15
					20
Cp6		Cp5		Fp6	25
DE	FL	DE	FL	DE	30
Fp8		Fp8		Fp8	35
C.E.	2340Z	C.E.	2352Z	C.E.	40
<del>AE</del>	03 JAN 95	<del>AE</del>	03 JAN 95	<del>AE</del>	45
					50
					55
					60

CTG 42.3  
 TG 42.3

DATE 03 JAN 95  
 SUPERVISOR FL  
 OPERATOR C.E.  
 PRIORITY  
 SUPERVISOR J.E.  
 VISUAL NO. 2328Z  
 032300Z JAN 95

PLATE NO. 12002

Sample Visual Message

Above is a sample visual message as received and retransmitted by USS SAMUEL B. ROBERTS (FFG-58/NSBR). Types of call signs authorized for use with visual communications are found in ACP 130, article 205.

Fp3 DE Fp8 T ZWL Dp2	FL	Fp6 DE Fp8 ZFH 2	SEM
<del>MB</del> <del>AEK</del>	1500Z 13 JAN 95	<del>MB</del> <del>AEK</del>	1600Z 13 JAN 95

Show all contents of procedure component exactly as transmitted Operator and Supervisor must insert own personal sign.	Show method of transmission Show TOD Date Month Year
---	--

Service Cross Message

Do not use the prosign IMI to obtain a message repetition after receipting for the message. Use an abbreviated service message employing the operating signal "ZDK" instead. (EX: INT ZDK 071902Z MAR 00 WB COMMENCE K.)

When an addressee desires to readdress a message to ships/stations not in the original address, use the operating signal ZFH1 (ACTION), or ZFH2 (INFORMATION), in the transmission instructions.

VISUAL MESSAGE  
 FORM 3110-20 (10-88) S/N 0107-LP-706-8000  
 Reorder from FPO Cpg. "1" stock point

CALL UP 07-XMT-A08 DE R07

BT					
CONFIDENTIAL	FILLER	SEE	COMM	CENTER	
FILE	FOR	TEXT	BT	0515Z	5
					10
					15
					20
					25
					30
					35
					40
					45
					50
					55
					60

TO: JOHN F. KENNEDY (CV-67)		DATE: 03 JAN 95	RELEASED BY:
TO: THIS TASK GROUP		OPERATOR: NBK	PRECEDENCE:
INFO: XMT JOSHUA HUMPHREYS (TAC-188)		OPERATOR: J.P.	SUPERVISOR: [Signature]
		INFO: 0532Z	VISUAL NO: 2
CLASS	C OF 1	CAPT	DOB
			9/2
		0515Z / 04 JAN 95	

Classified Message Filler

VISUAL MESSAGE  
 OPNAV FORM 2110-30 (10-58)  
 Reorder from FPM's Cog "I" stock point S/N 0107-705-8000

CALL UP		Fp8 DE Cp6	
HEADING			
P 041915Z JAN 95 FM 1p3 TO 8p2			
GR7 BT			
UNCLAS	THIS	MESSAGE	FOR
USE	ONLY	BT	K
			SAMPLE
			5
			10
			15
			20
			25
			30
			35
			40
			45
			50
			55
			60
FROM: CTG 42.3		DATE: 04 JAN 95	RELEASED BY: B
TO: TU 42.3.2		SYSTEM: FL	PRIORITY: PRIORITY
INFO:		OPERATOR: D.P.	SUPERVISOR: J.P.
TAG: C OF S CAPT OOD COMM. CEN.		TOP: 1925Z	VISUAL INL: 3
		041915Z JAN 95	

PLATE NO. 12602

Message received and readdressed by USS SAMUEL B ROBERTS (FFG-58/NSBR).

**NOTE: Readdressal releasing signature and multiple service cross.**

The address component of a codress message is encrypted within its text unless the message contains address indicating groups (AIG'S). The requirement to handle these messages visually within the U.S. Navy is almost non-existent because of the crypto systems in use. There may however be an occasional requirement to relay a Codress message between allied ships using procedures contained in ACP 130.

Service messages, like all Allied Naval visual messages, should be prepared and transmitted in plaindress, abbreviated plaindress, or codress form. These messages are normally transmitted and/or received by telecommunications facility personnel, but may also be handled visually. Examples of plain language service messages:

- (1) Plaindress format:  
 P 022000Z JAN 97 GR9 BT

UNCLAS SVC TGO DOWN COME  
UP PRI-TAC CIRCUIT 277.8  
BT K

- (2) Abbreviated plaindress format:

BT UNCLAS SVC TGO  
DOWN COME UP PRI-TAC  
CIRCUIT 277.8 BT  
2000Z K

An abbreviated service message contains only prosigns, operating signals, address designators, parts of messages, and other data as necessary to identify a particular message. Example:

- (1) INT ZDK 021500Z JAN 97 K

- (2) Abbreviated plaindress format:

BT INT ZDK  
NBZO 021500Z JAN 97 ZAR2  
BT 2000Z K

- (3) Plaindress format:

P 022000Z MAR 00 GR6 BT  
INT ZDK 021500Z MAR 00  
ZAR3 BT K

**NOTE:** The abbreviated service message shown in example (1) is not logged because it does not contain the long break or DTG/TG in the heading/ending. Further explanation of service and abbreviated service messages is contained in ACP 130.

### Visual Station File

The visual station file contains all outgoing and incoming messages, (except signals and service messages which do not contain the prosign "BT") handled visually. It includes either the original copy of unclassified messages or filler for classified ones. These messages/fillers should be filed in date-time-group order.

Onboard a flagship, if the embarked flag so desires, a separate visual station file will be maintained for flag traffic. If separate ship and flag files are maintained, it is important to note that any message filed in the embarked flag's file must, if the address so indicates, also be filed in the ship's file.

Retain and dispose of the visual station file per SECNAVINST 5212.5 (Disposal of Navy and Marine Corps Records). The retention period for the visual station file is 30 days.

## Visual Communications Log

The visual communications log is a ledger type record book or other bound book specifically printed for this purpose. The visual log shall contain a complete, accurate, chronological record of all visual traffic sent and received by the command except ZWC traffic and service messages which do not contain the prosign "BT". Because the visual log is a legal document subject to review by Court of Inquiry, its proper safeguarding and maintenance is of extreme importance.

The visual log shall be safeguarded and maintained by the signal watch supervisor when the visual watch is set, and by the duty Quartermaster, or person qualified as the duty Quartermaster, when the visual watch is not set. A daily visual log will be kept.

Prior to assigning any security classification to the visual log, consult SECNAV M-5510.36.

Retain and dispose of the visual log per SECNAVINST 5212.5 (Disposal of Navy and Marine Corps Records). Maintain the visual log for 30 days after final entry. At decommissioning, dispose of the log immediately provided it does not violate SECNAVINST 5212.5.

Common usage determines the guidelines for visual log entries. It is not feasible to try to document guidelines for every situation which may occur. If this chapter does not cover a particular situation, the watch supervisor or duty Quartermaster should use his/her own best judgment to decide what to enter. The following gives some ground rules for use in a visual log:

(1) Use black ink;

(2) Print legibly. Print letters, numerals, flags, pennants, substitutes, and tack lines using Chapter 1 Figure II of ACP 130 as a guide, with the following modifications:

Juliett                      Place horizontal across top of J

Zulu                         Slash (Z)

Zero                         Slash through zero (0)

Numeral one                Place horizontal across bottom

Numeral nine               Straight vertical (9)

Group/Flotilla            GROUP or FLOT, whichever applies

(3) Leave no blank spaces between lines;

(4) Draw single line through error and insert personal sign at left of page on the line of entry;

(5) Close out page at 2359Z each day. End the page with: "END ZULU DAY, WATCH CONTINUED;" N/A when visual watch is not set.

(6) Begin new page at 0001Z each day. Begin with 0001Z: "BEGIN NEW ZULU DAY, WATCH CONTINUED;" N/A when visual watch is not set.

(7) Sign in when assuming watch/duty. Example: "ASSUMED THE WATCH/DUTY" and signature should be on the same line;

(8) Sign out when relieved of watch/duty. Example: "WATCH RELIEVED BY SM3 FLAGS" and signature should be on separate lines;

(9) Enter all traffic (except ZWC traffic and service messages which do not contain the prosign "BT"), and include day shapes, exchange of calls, casualties to personnel or equipment, setting/securing visual watch, time zone changes and any other events pertaining to visual communications;

(10) Lengthy plain language addresses denoting task organizations may be converted to special task organization call signs prior to entry, e.g., CTE 50.1.1.1 converted to 3p1 (within own task organization);

(11) Use local time to indicate watches (00-04, 20-24, etc).

The visual log shall include the following entries:

1. DATE: GMT date, followed by time zone.
2. TIME: All times, except for local watch times, GMT. (0000Z is not used).
3. TOR/AD:
  - a. Incoming morse/sem: Time of receipt.
  - b. Incoming flaghoist: Time signal or ANS hoisted at the dip.
  - c. Outgoing flaghoist: Time signal hoisted at the dip, e.g., H1, speed flags.
  - d. Time of plain language entries.

e. Time prep is dipped to observe colors.

4. TOD/CU

a. Outgoing morse/sem: Final TOD. Note that an outgoing message should be logged only once. Show interim TODs for multiple deliveries in the service cross.

b. Incoming flaghoist (flaghoist which has been closed up by units for which you are responsible) and ANS: Time own ship closes up.

c. Outgoing flaghoist: Time own ship closes up.

d. Sunrise, morning and evening colors: Time own ship answers PREP close up.

5. TOX/HD

a. Morse: Time of execution of executive method message.

b. Flaghoist: At time signal is returned to deck. (This may or may not be moment of execution - see ACP 130, article 810.) Recommend separate entries for those signals in ATP 1, Vol II which are executed when placed at the dip after flying close up. For successive signals from PUB 102, enter time ANS is dipped instead of hauled down. (See PUB 102, pg 1-5.)

6. METH: Method of transmission. For outgoing Morse/semaphore traffic using multiple methods of transmission, enter method used for final TOD. The following abbreviations are used within the Navy to denote methods of visual transmission:

a. FL: Small signal searchlight

b. SL: Large signal searchlight

c. BK: Yardarm blinkers

d. NFL: Infrared directional

e. NBK: Infrared non-directional

f. SEM: Semaphore

g. FH: Flag hoist

h. MPL: Multi-purpose light

7. RCVD FROM: Show call sign of ship from which traffic is received. The ship's visual call sign (VCS) is used in most cases, however; if the VCS is the same for different units, which is possible when task organization consists of combined U.S./Allied units, or if ship is not assigned a VCS (merchant and non-allied naval units), use international call sign (ICS). If ICS cannot be determined, show other identifying data in "remarks" section, (nationality, hull number, name, etc).

8. TRANS TO: Use VCS or ICS as described above. Enter call sign of ship receiving final delivery of Morse/semaphore traffic. Show call signs for interim deliveries in message service cross. When relaying a flag hoist signal, enter call sign of ship which answers signal, either to assume relay responsibility or as addressee. For signal originated by own ship requiring an answer, enter:

- a. Call sign of individual ship(s) addressed;
- b. Call sign of ship assuming relay responsibility; or,
- c. If originator is in direct communications with all addressees, a collective or command call sign may be used.

9. ORIG/ACT/INFO/XMT: Put call sign(s) in each column where applicable. Log all call signs as received/transmitted.

10. TRAFFIC IN/OUT/REMARKS

- a. Incoming/outgoing Morse/semaphore: Enter message DTG MO YR or TG as applicable. If unable to obtain time group (file time) from non-allied warships or merchant ships, enter own TOR in this column to be used as reference for visual station file.
- b. Incoming/outgoing flag hoist: Enter entire heading including substitutes when used to modify heading and text for both relay and non-relay signals. Convert substitutes in the text of signals to flag/pennant they are representing.
- c. VIS NR: Using a visual number is a convenient method of accountability. After placing the original or filler in the visual station file, circle the visual number to indicate all routing and relay (if required) has been completed. Start new visual numbers at the beginning of each new month.



TASK ORG	TASK ORGANIZATION DESIGNATION/ASSIGNED UNITS	SPECIAL TASK ORG CALL SIGN	VISUAL CALL SIGN	INTL CALL SIGN
CTG 42.3	CDR TASK GROUP	1p3	p0p7	
TG 42.3	TASK/BATTLE GROUP	7p3	p7	
CTU 42.3.1	CDR CARRIER GROUP	2p1	p0p3p7/p0p8	
TU 42.3.1 (F) (FF)	CARRIER GROUP JOHN F KENNEDY (CVN-67)	8p1	p3p7/p8 Rp6p7	NJFK
CTU 42.3.2	SCREEN CDR	2p2	p0p5/p0p8	
TU 42.3.2 (F)	SCREEN LEAHY (CG-16) SAMUEL B ROBERTS (FFG-58) LEYTE GULF (CG-55) REED (FFG-30)	8p2	p5/p8 Cp1p6 Fp5p8 Cp5p5 Fp3p0	NWDL NSBR NLEG NSLR
CTU 42.3.3	CDR REPLENISHMENT FORCE	2p3	p0p7p2/p0p8	
TU 42.3.3 (F)	REPLENISHMENT FORCE SYLVANIA (AFS-2) JOSHUA HUMPHREYS (TAO-188)	8p3	p7p2/p8 Ap2 Ap1p8p8	NMYU NNJH

**TASK BOARD ORGANIZATION**

CALL UP Ep8

BT					
UNCLAS	THIS	MESSAGE	FOR	SAMPLE	
USE	ONLY.	BT	2206Z	K	5
					10
					15
					20
					25
					30
					35
					40
					45
					50
					55
					60

FROM: SCREEN COMMANDER					DATE: 04 JAN 95	RELEASED BY:
TO: SAMUEL B. ROBERTS (FFG-58)					SYSTEM: FL	PRIORITY:
					OPERATOR: J.P.	SUPERVISOR: W.J.
INFO:					TO: 2221Z	VISUAL NO.: 4
LAB:	C OF S:	CAS: B	ODD: K	COMM. CEN: J.P.	INFO: 2206Z / 04 JAN 95	

PLATE NO. 12602

Abbreviated Plaindress Message received by the Samuel B. Roberts (FFG-58) with the call serving as the address.

**NOTE:** When an abbreviated call is used, the message is addressed from and to the senior officer embarked.

The sample visual log below shows examples of visual log entries. Note that even though the visual watch is not set, all official traffic must nonetheless be logged.

## VISUAL LOG

DATE 01 JAN 95

TIME ZONE +8 U

TOX A/D	TOX O/U	TOX H/B	METHOD	RECEIVED FROM	TRANS TO	ORIG	ACTION ADEE	INFO ADEE	XMT ADEE	TEXT OR DATE TIME GROUP	VIC NR
	1425	1430	FH	Rp7		p8p4				PREP	
	1430	1630	FH			Fp8				3RD	
	1555	1600	FH	Rp7		p8p4				PREP	
1605										DUTY SM RELIEVED BY SM <sup>2</sup> HAWK C.E. Archer SM <sup>3</sup>	
1605										ASSUMED DUTY SM J.P. Hawk SM <sup>3</sup>	
	1709	2203	FH			Fp8				COOB A	
	2310	0230	FH			Fp8				3RD	
	02 JAN 95 (+8)										
	0225	0230	FH	Rp7		p8p4				PREP	
	1424	1429	FH	Rp7		p8p4				PREP	
	1429	1608	FH			Fp8				3RD	
	1555	1600	FH	Rp7		p8p4				PREP	
1605										DUTY SM RELIEVED BY SM <sup>2</sup> RICKS J.P. Hawk SM <sup>3</sup>	
1605										ASSUMED DUTY SM J.P. Hawk SM <sup>3</sup>	
	1615	2110	FH			Fp8				B	
	1617	2110	FH			Fp8				11	
	03 JAN 95 (+8)										
	0100	0231	FH			Fp8				3RD	
	0226	0231	FH	Rp7		p8p4				PREP	
	1423	1428	FH	Rp7		p8p4				PREP	
	1428	1530	FH			Fp8				3RD	
	1555	1600	FH	Rp7		p8p4				PREP	
1610			FL	Rp7		p8p4	Fp8			PREP ED49-T09U	
1630										DUTY SM RELIEVED BY SM <sup>1</sup> GRAY	

CONFIDENTIAL (When filled in)

## Sample Visual Log

THIS LOG IS CLASSIFIED FOR ILLUSTRATION PURPOSES ONLY

NOTE: Information signals originated by other units are not required to be logged, but recommended. Logging of these signals shall be left to the discretion of the Leading Quartermaster.

\* HP 4760 FROM MERCHANT MARINE SHIP IDENTIFICATION GUIDE and (NIC-2050G-001-90)

**THIS PAGE INTENTIONALLY BLANK**

APPENDIX HCOMMUNICATIONS INSTRUCTIONS AND PROCEDURES  
FOR NAVAL ACTIVITIES COMMUNICATING WITH  
US FLAG MERCHANT SHIPS (MERSHIPS)  
GENERAL INFORMATION**General**

This section provides instructions and procedures for Naval activities to communicate with U.S. Flag Merchant Ships (MERSHIPS) per CNO policy.

Because there is no single structured method or capability for communicating with MERSHIPS, this section describes MERSHIP/commercial record carrier capabilities and the established procedures for Naval activities to communicate with MERSHIPS.

The Navy has no system specifically designated for communications with MERSHIPS. The limited Navy ship/shore facilities currently in operation provide communications support primarily for ships under the control of the Military Sealift Command (MSC). The Navy relies mainly on the following capabilities to communicate with MERSHIPS:

(1) Coast Guard COMMSTA ship/shore and broadcast; ARQ/Simplex Teleprinting Over Radio (SITOR). This is an automatic repeat, error-correcting high frequency radio teletype system which is also called Narrow Band Direct Printing (NBDP) CR radiotelex or simply HF-RATT;

2) Commercial carriers such as COMSAT General, who provide maritime satellite services via the international maritime satellite organization.

While increasing numbers of MERSHIPS are being equipped with INMARSAT voice/record communications terminals and SITOR systems, a significant number of them have only CW and MF/HF voice communications capability. Also MERSHIPS ordinarily do not carry crypto systems. All government or government-contract classified and unclassified national security-related information transmitted via INMARSAT, i.e., all official business, must be encrypted. Per DOD and Navy policy, encryption devices must be National Security Agency (NSA) approved cryptographic equipment, e.g., STU-III, GILLAROO, KG-84, ANDVT, which provide protection from exploitation by unauthorized intercept. Additionally, due to the costs associated with delivering messages via commercial carriers, messages must be as brief as possible.

Navy originated message traffic, which is commercially refiled for delivery to MERSHIPS, is generally grouped into two categories because processing requirements differ in each case.

(1) The first category is the General Emergency Message originated by the Chief of Naval Operations (CNO) to advise MERSHIPS of mobilization or that the United States is at war. This message is identified in the Defense Mapping Agency Hydrographic Topographic Center publication 117 (series). It is assigned a FLASH precedence (urgent signal XXX) and must be delivered to all MERSHIPS via the most expeditious means available. Special handling is required. Procedures are described below.

(2) The second message traffic category is that operational traffic originated by other Naval commands throughout the world and addressed to any of the ships in the merchant fleet. This traffic is routed per established DOD routing doctrine and commercially refiled with commercial record carriers. Procedures for routing and delivering operational traffic are described in subsequent paragraphs of this chapter.

Messages addressed to MERSHIPS are delivered via commercial coastal radio stations using SITOR or via INMARSAT systems. Procedures for communicating with MERSHIPS via INMARSAT are described under International Maritime Satellite Communications System procedures paragraph. U.S. coastal stations, which operate SITOR communication is identified in the U.S. Merchant Marine/U.S. Navy Communications Call-Up Procedures in Emergency Situations paragraph.

INMARSAT ID numbers are for official use only (FOUO). To provide access control for Navy ships and prevent INMARSAT terminals from being inundated with unofficial phone traffic, distribution of a list of INMARSAT ID numbers is limited to Fleet and Type Commanders. INMARSAT ID numbers are not to be released outside of U. S. Government channels without authorization from appropriate Fleet Commanders or Service Headquarters.

### **CNO General Emergency Message Procedures**

#### GENERAL.

In the event of the declaration of a state of war or a national emergency, merchant vessels of the United States and those foreign flag vessels which are considered under effective United States control will be subject to control by agencies of the United States Government. Appropriate agencies of the Maritime Administration (MARAD) of the Department of Transportation will allocate and employ such merchant vessels and allocate domestic port facilities, equipment, and services. The Coast Guard will coordinate the movement of merchant ships within domestic ports and dispersal anchorages. Appropriate Naval commanders, through the Naval Control of Shipping Organization (NCSORG), will control the movement, routing and diversion of merchant ships at sea.

The Chief of Naval Operations (CNO) will announce a state of war or a national emergency to merchant ships in a plain language

emergency message. This message will be broadcast through available commercial and military communications systems. The message will place merchant vessels of particular types under United States control and will direct them to comply with instructions in Chapter 8 of the Defense Mapping Agency Hydrographic Topographic Center (DMAHTC) publication 117 (series) (Radio Navigational Aids).

Appropriate authority may direct these procedures be followed during Naval Control of Shipping exercises.

#### MESSAGE INITIATION PROCEDURE

The CNO Duty Officer will initiate the CNO General Emergency Message, which will contain a special accounting code "CNO NA". This code indicates to commercial communications systems, namely the International Telegraph and Telephone Company (ITT) and Radio Corporation of America (RCA) that this message is to be handled at "no charge". Based upon a 1976 FCC ruling ITT and RCA have agreed that the CNO General Emergency Message and like emergency messages transmitted during Naval exercises can be accepted and broadcast to MERSHIPS by associated coastal stations free of charge. An exception to this free service, however, will be made if messages are transmitted via American Telephone and Telegraph (AT&T) and MCI affiliated Radio Manila stations "DZG" and "DZR". Normal charges will accrue in these cases since these foreign government stations are not bound by the FCC rule. On receipt of messages containing the symbol "CNO NA", operating personnel at the ITT and RCA Washington Operations Centers can immediately call the CNO Duty Officer at the Pentagon, at their option, to verify the authenticity of the message. After such coordination, ITT and RCA Operations Center personnel will forward the message to coastal stations and INMARSAT entry stations, as appropriate, for broadcast to MERSHIPS.

The address "ALL US CONTROLLED MERCHANT SHIPS" is a Collective Address Designator (CAD) for message routing purposes. The heading and general contents of the CNO General Emergency Message will be similar to the example below:

FLASH

(DATE-TIME GROUP)  
 FM COMNAVNETOPSCOM WASHINGTON DC//N32/N31/N3//  
 TO COGARD CAMSLANT CHESAPEAKE VA//OO//  
 COGARD CMASPAC PT REYES CA//OO//  
 COMCOGARD MARSEC GU  
 COGARD COMMSTA KODIAK AK//OO//  
 COMDT COGARD WASHINGTON DC//HSC-4T//  
 COMLANTAREA COGARD PORTSMOUTH VA//AT//  
 COMPACAREA COGARD ALAMEDA CA//OO//  
 COMPSRON TWO//  
 MARITIME ADMIN WASHINGTON DC// MAR 745//  
 NCTAMS LANT NORFOLK VA//3514W/3514/35/351//  
 NAVCOMTELSTA DIEGO GARCIA//N3//

NCTAMS PAC HONOLULU HI//N5/N5131/N33//  
 NCTAMS EURCENT NAPLES IT//N63//  
 NAVCOMTELSTA GUAM GU//80//  
 COMSCLANT BAYONNE NJ//  
 COMSCPAC OAKLAND CA//  
 COMSCFE YOKOHOMA JA//  
 COMSCEUR LONDON UK//  
 COMPSRON THREE//  
 COMPSRON ONE//  
 INFO CNO WASHINGTON DC//N61//  
 CINCLANTFLT NORFOLK VA//N3/N6//  
 CINCPACFLT PEARL HARBOR HI//N5//  
 CINCUSNAVEUR LONDON UK//N6//  
 COMSC WASHINGTON DC//N67//  
 NAVCOMTELSTA WASHINGTON DC//N3//  
 BT

UNCLAS //N00000//  
 MSGID/GENADMIN/CNO//  
 SUBJ/GENERAL EMERGENCY MESSAGE//  
 RMKS/1. UNITED STATES AT WAR WITH \_\_\_\_\_ . MASTERS OF  
 U.S.CONTROLLED MERCHANT SHIPS COMPLY WITH INSTRUCTIONS CONTAINED  
 IN CHAPTER EIGHT ENVELOPE ALFA OF DEFENSE MAPPING AGENCY  
 HYDROGRAPHIC CENTER PUB 117, ON RECEIPT.//

EXAMPLE OF CNO GENERAL EMERGENCY MESSAGE

The CNO Duty Captain shall release the message to the OPNAV TCC who in turn shall route the message via the Automatic Digital Network (AUTODIN) to the fleet commanders, all NCTAMS, NAVCOMTELSTA'S, COAST GUARD CAMSLANT, CHESAPEAKE, VA, CAMSPAC PT REYES, COMMSTA'S and MARAD for transmission to all U.S. controlled merchant ships as indicated below.

A routing profile has been established to deliver the CNO General Emergency Message via AUTODIN to Naval Coast Guard CAMSLANT, CHESAPEAKE, VA, CAMSPAC PT REYES, CA AND COMMSTA KODIAL, AK for further transmission to merchant ships by all available military and commercial communications systems. NCTAMS and NAVCOMTELSTA'S will automatically route the emergency message to the common channels of satellite broadcasts via NAVCOMPARS. For other broadcasts and circuits the message must be routed and transmitted as described below.

BROADCAST PROCEDURES. Each of the communications commands listed above will broadcast the CNO General Emergency Message per the following procedures.

NCTAMS/NAVCOMMSTA/NAVCOMTELSTA

(a) Where required to guard 500 kHz by Communications Operating Requirements (COR), broadcast the emergency message every hour for 24 hours. Commence transmission of the message during the last 30 seconds of the first silent period.



(b) On all active single channel broadcasts, transmit the emergency message at the beginning of each schedule or every hour for a 24-hour period.

#### COAST GUARD COMMSTA'S

The emergency message will be routed via DTH to Coast Guard CAMSLANT, CHESAPEAKE, VA, CAMSPAC PT REYES, AND COMMSTA Kodiak AK.

These stations will transmit the emergency message via NAVTEX broadcast on 518 kHz immediately upon receipt and each scheduled broadcast thereafter.

Each COMMSTA will transmit the emergency message on SITOR, ship/shore and mobile maritime and public correspondence circuits as applicable.

#### **Routing Record Messages To Mershops**

General. MERSHIPS engaged in foreign commerce are required by law to report their positions every 48 hours while underway and when entering and departing port using the U.S. Flag Merchant Vessels Location Filing System (USMER). Per request of the U.S. Maritime Administration (MARAD), Masters and Radio Officers of MERSHIPS should include the primary and local geographic radio stations being guarded in the remarks section of their USMER reports. MERSHIPS sends these reports to the Naval Marine Intelligence Center (NAVMARINTCEN), who provides the information to the U.S. Coast Guard for their Automated Mutual Assistance Vessel Rescue (AMVER) system. AMVER, described in detail in paragraph 631 of this publication, is a voluntary participatory computerized system for maintaining the positions of participating merchant vessels and is used for search and rescue purposes.

LOCATING ROUTING INFORMATION. The U.S. Military Communications-Electronics Board (USMCEB) has designated the Naval Computer and Telecommunications Area Master Station, Pacific (NCTAMS PAC) the DOD central routing authority for messages addressed to MERSHIPS. To ensure proper routing and delivery of messages to MERSHIPS, all Naval activities should send record traffic to NCTAMS PAC for further routing to MERSHIPS unless they have other positive message routing information available.

Routing information for ships controlled by the Commander, Military Sealift Command (COMSC) is available per the procedures described in COMSCINST 2000.2.

NCTAMS PAC uses the following standard operating procedures to obtain communications routing information for MERSHIPS not under COMSC control.

The NCTAMS' database operator will request the routing

information from the NAVMARINTCEN Merchant Analyst, DSN 293-2106 or Commercial (301) 763-2106. NAVMARINTCEN will provide information from its radio guard database, which is updated by information taken from ships' AMVER reports. If NAVMARINTCEN is unable to provide the requested information,

The NCTAMS' database operator will then call Commander, Military Sealift Command (COMSC) in Washington, D.C. (during working hours only) DSN 288-2666 or commercial 202-433-2666 to request any routing information available on the merchant vessel.

If routing information is not available from COMSC, the NCTAMS' database operator will then attempt to locate the ship by requesting information on the ship's owner from MARAD during working hours.

MESSAGE DELIVERY TO MERSHIPS. NCTAMS, upon determination of the best known routing, will forward messages for delivery. Established DOD communications doctrine permits traffic to be delivered via AUTODIN to the commercial refile station nearest the coastal station transmitting traffic to the ship. Because complete information is not always available within government channels as to what station is serving a particular ship, it is often difficult to achieve positive message routing. Consequently, messages addressed to merchant ships are sometimes delayed. To improve this situation, the FCC has ruled that record carriers should improve the alternate route capability and interconnectivity between coastal stations for final delivery by transmission to ships. Better interconnectivity between coastal stations will improve traffic delivery to merchant ships. Messages can then be directly routed to another coastal station for transmission in the event a ship did not establish contact with a primary calling station. The record carriers also reserve the option of using either INMARSAT or the coastal stations to deliver messages to merchant ships at sea. However, when it is known that a U.S. Flag Merchant Ship is guarding INMARSAT, the INMARSAT procedures detailed below may be used for message delivery.

### **International Maritime Satellite Communications System (INMARSAT) Procedures**

GENERAL. The 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, which is headquartered in London, UK. COMSAT operates INMARSAT earth stations in the United States at Southbury, Connecticut and Santa Paula, California and overseas at Ata, Turkey to provide worldwide commercial satellite services over INMARSAT.

To ensure rapid and reliable communications are available when needed, the Chief of Naval Operations (CNO) has directed that procedures be established to permit Naval commands to communicate

with MERSHIPS via commercial maritime satellite systems. Naval commands are authorized to communicate with MERSHIPS via INMARSAT using the procedures outlined below. Per CNO direction, INMARSAT will be used to communicate with MERSHIPS for transmission of emergency messages and messages pertaining to fleet support operations only. Routine operational, administrative, hydrographic and navigational area warning messages will be transmitted by Naval commands to MERSHIPS via INMARSAT at the discretion of the Officer in Tactical Command (OTC). INMARSAT services are available to MERSHIPS and all others operated under the control of COMSC.

#### **Communications With U.S. Flag Merships Via SITOR**

The Navy relies on the Coast Guard to provide a real time communications interface with MERSHIPS. The use of HF SITOR, also called Narrow Band Direct Printing (NBDP) CR radiotelex, is the U.S. and international standard means for ship-shore-ship unclassified record message send and receive. The Safety of Life At Sea (SOLAS) convention, as amended by the Global Maritime Distress and Safety System (GMDSS) 1988 amendments, requires SITOR to be on all ships not having INMARSAT ship earth stations. SITOR is now the standard for unclassified terrestrial data and message communications to ships. It replaces unclassified radio teletype (RATT) for this purpose.

Coast Guard telecommunications facilities presently equipped with SITOR are COGARD CAMSLANT (NMN), COGARD CAMSPAC (NMC), and COMMSTA Kodiak (NOJ)

CNO has validated the need for interconnecting circuits between Coast Guard COMMSTAS and Naval communication stations in support of communications with U.S. Flag Vessels. Connectivity now exists between the following:

- (1) COGARD CAMSPAC PT Reyes, CA and NAVCOMTELSTA Sand Diego, CA.
- (2) COGARD CAMSLANT Chesapeake, VA and NCTAMS LANT, Norfolk VA.

In determining the use of Coast Guard HF SITOR equipment to support emergency communications with U.S. Flag Vessels, the following points were considered: the SITOR equipment at Coast Guard COMMSTAS is used on a daily basis which ensures that operators are trained on the equipment and its use, the operating condition of the equipment is known at all times; the equipment is supportable through the Coast Guard Electronic Maintenance System.

#### **Allied Merchant Ship Communications Systems (MERCOMMS)**

A new Allied Merchant Ship Communications System (MERCOMMS) is evolving in the Allied Nations Communications Agency (ANCA) to

improve allied protection of merchant shipping in time of war under the Naval Control of Shipping Organization. Merchant ship message routing responsibilities in MERCOMM will be relatively the same, except that Ocean Control Authorities (OCA) in the NCSO will be responsible for message delivery to allied merchant ships in assigned ocean areas, using specifically designated military, Coast Guard, and commercial communications facilities.

Pending the availability of MERCOMMS, communications with merchant ships under stressed conditions are as outlined in ACP 149 and Defense Mapping Agency DMAHTC 117 A & B (series) publications.

**U.S. Merchant Marine/U.S. Navy Communications Call-Up Procedures In Emergency Situations**

CNO established the following procedures to ensure that U.S. Flag and U.S. Controlled Fleet merchant ships may quickly establish communications with U.S. Navy commands via INMARSAT and HF radio. These procedures were implemented by CNO ltr 2099 Ser 941C/BU535705 of 31 May 88. It is essential that personnel in command centers, ashore communications facilities and surface units are familiar with these requirements and procedures in order to respond to merchant ship requests for Navy assistance.

The following situations warrant immediate use of emergency communications for MERSHIPS requesting assistance from the U.S. Navy.

(1) Attacks, threats of attack or hostile actions by military forces. This includes warning shots and/or observation of mining operations in international waters, as well as actual attack.

(2) Harassment by military forces, including threats or attempts of boarding and seizure or hostage taking.

(3) Terrorist attack/threat of terrorist attack or seizure.

(4) Piracy

(5) Rescue in event of natural disaster if no acknowledgment is received from use of established distress and safety communications procedures.

Emergency communications from merchant ships in crisis situations essentially involve incident reporting and requests for USN protection/assistance on a real time basis. Submit requests for assistance to Navy Fleet Command Centers by either INMARSAT or HF media.

Below is a listing of commercial telephone numbers for Fleet Command Center, Naval Communication Stations and USCG Communication Station with their areas of command and/or

communications coverage.

EMERGENCY AREA PHONE NUMBERS

Ocean Area	Command Name	Telephone	Telex
Mediterranean , Baltic, Mid East	CINCUSNAVEUR	044-1-409-	
	OPCONCEN London UK	4479/4473/4527* From CONUS: 011-44-1- 409-XXXX	
	NCTAMS EURCENT Naples IT	039-81-760-6343 From CONUS: 011-39- 81-760-6343	127-775
	COMLANTAREA COGARD Portsmouth, VA	(757) 298-6246	
Atlantic, Caribbean, Atlantic Approaches to Panama Canal, North Sea	CINCLANTFLT OPCONCEN Norfolk, VA	(804) 444-6602, 445- 5582	
	NCTAMS LANT Norfolk VA	(804) 444-2150, 444- 7111	
	COMLANTAREA GOGARD Portsmouth, VA	(757) 398-6246	127-775
	COGARD CAMSLANT Chesapeake VA	(757) 421-6240	
Eastern Pacific, Mexico, Central America	CINCPACFLT OPCONCEN Pearl Harbor, HI	(808) 471-3201, 422- 5944	
	NCTAMS PAC Honolulu HI	(808) 653-5544, 653- 5303	
	NAVCOMTELSTA San Diego CA	(619) 239-9381 thru 9385	72-343
	COMPACAREA COGARD San Francisco, CA	(510) 437-3700	
	COGARD COMMSTA Kodiak, AK	(907) 487-5778	
	COGARD COMMSTA Point Reyes, A	(415) 669-7409	
Mid Pacific, Northern Pacific, Pacific Approaches to Panama Canal, South America	COGARD MARSEC, GU	011-672-355-5653	

Ocean Area	Command Name	Telephone	Telex
Western Pacific, South	CINCPACFLT OPCONCEN Pearl Harbor, HI	(808) 471-3201, 422-5944	
	<b>Emergency Area Phone Numbers</b>		
	NACOMTELSTA Guam, GU	011-671-355-5373	
	NAVCOMTELSTA FAR EAST YOKOSUKA JA	011-0468-26-1911, Ext 7497	
Pacific, Southeast	COGARD MARSEC, GU		
Asia, Straits of Malacca, Sea of Japan, Indian Ocean	COGARD COMMSTA Kodiak, AK	011-672-355-5653  (907) 487-5778	
Persian Gulf, Red Sea	CINCLANTFLT/CINCUSNA VCENT OPCONCEN (For Ships in Persian Gulf)	(808) 471-3201, 422-5944	
	NACOMTELSTA Guam, GU	011-671-355-53475/5376	
	COGARD MARSEC, GU (For Ships in Red Sea)	011-672-355-5653	INMARSAT ID #150-1733
	NCTAMS EURCENT Naples IT	0039-81-760-6343 Form CONUS 011-39-81-760-6343	127-775
		(757) 398-6246	
	COMLANTAREA GOGARD Portsmouth, VA		

#### Emergency Area Phone Numbers

Navy communications facilities with FLTSATCOM interface capability will, on direction from FLTCOM OPCONCEN's, place calls to the following Navy communication stations which have a conference bridge capability to establish unclassified ship-to-ship voice connectivity with Navy afloat units via Navy FLTSATCOM systems.

NCTAMS LANT NORFOLK VA (804) 444-2150, 444-7111

NCTAMS PAC HONOLULU HI (808) 653-5549

NCTS GUAM GU 011-671-5511

NCTS NAPLES IT Does not have interface capability.

Procedures for emergency incident reporting and/or requests for USN assistance emphasize use of voice communications between the

merchant ship and the commands/facilities ashore and afloat. However, record communications should also be used when appropriate. MERSHIPS are authorized to use frequencies allocated to FLTCOM High Command Worldwide Voice Network (HICOM) to enter the net to pass emergency traffic.

g. Merchant ships will use the following voice call-up procedures if an indefinite call-up address is to be used:

"ANY NAVY/AIR FORCE/COAST GUARD STATION GUARDING THIS NET, THIS IS SS EXAMPLE, EMERGENCY MESSAGE FOLLOWS."

Merchant ships are cautioned that Navy shore stations and/or afloat units guarding HICOM or other tactical HF nets may respond with an alpha-numeric daily changing call sign and advise the merchant ship to send traffic. The Navy unit will not reveal its name to prevent compromising the call sign.

h. Merchant ships equipped with INMARSAT will attempt to direct dial the appropriate FLTCOM via the listed telephone numbers above to report an incident. If the call cannot be completed via direct dial, they will place the call via the INMARSAT operator who will attempt to contact the OPCONCEN. If the call cannot be completed in this manner, merchant ships will then dial the appropriate Naval Telecommunications facility for patch or relay to the FLTCOM OPCONCEN. If contact cannot be made via the NCTAMS/NAVCOMTELSTA, merchant ships will request the INMARSAT operator to place the call to the U.S. Coast Guard Area Operations Centers who will notify the FLTCOM. U.S. Flag or effective U.S. controlled merchant ships operating in the North Arabian Sea/Persian Gulf area requiring assistance from USN ships of Joint Task Force Mid East should call NCT GUAM GU to patch the call.

i. When using HF, the merchant will first contact FLTCOM OPCONCENS via the HF Public Coast Radio Station, giving information in prescribed format noted earlier in this appendix. If contact cannot be made, the MERSHIP will call the closest NCTAMS/NAVCOMTELSTA, USAF Communications Station or U.S. Coast Guard Communications Station to relay the request to the appropriate OPCONCEN. MERSHIP-to-Navy communication may also be initiated for initial call-up on 2182 kHz or one of the Navy HICOM or tactical frequencies. However, FLTCOM OPCONCEN must approve establishing extended ship-to-ship communications between merchant ships and USN afloat units in advance. Emergency messages may also be transmitted over the International Distress frequency (500 kHz) and should be addressed to Coast Guard or private sector stations, with request for relay of messages to Navy OPCONCENS.

Merchant ships which use HF SITOR/Narrowband Direct Printing (NBDP) or CW record communications send traffic to the Coast Guard Communications Station or Public Coast HF Radio station(s) normally providing record communications support services.

INMARSAT equipped ships file voice or TELEX traffic via appropriate earth stations. Emergency/distress messages received by non-US navy facilities will be immediately forwarded to the appropriate Navy Command center.

Merchant ships will use the following format for brevity and uniformity in reporting incidents:

To: Fleet Commander Command Center (as appropriate)

Name of Ship - International Call Sign

Position: (Latitude/Longitude) Date and Time: (ZULU TIME)

Brief Description: (Military attach, seizure, etc)

EXAMPLE:

TO: CINCPACFLT COMMAND CENTER

- A. SS NOGALES
- B. KCSD
- C. LAT 05N, LONG 105E
- D. 231800Z JAN 00
- E. SHIP UNDER ATTACK BY MACHINE GUN AND RIFLE FIRE, ETC.

Upon receipt of an emergency transmission by the OPCONCEN the FLTCOM will determine what action will be taken, e.g., dispatch of forces, establishing direct communications between the merchant ship and Navy afloat unit, providing guidance. Decision factors affecting Navy response are contingent upon availability of USN units, proximity of them to the merchant ship, and Rules of Engagement applicable to the theater of operations. The FLTCOM OPCONCEN may consider it essential for the merchant ship to establish direct non-secure voice communications with U.S. Navy surface units. If so, it will direct the merchant ship to call the appropriate NCTAMS for a patch to the Navy ship(s) by use of voice conference bridge between the commercial media (INMARSAT, HF) and the Navy's Fleet Satellite Communications (FLTSATCOM) system (for those ships that do not have INMARSAT). If direct HF voice connectivity between the merchant ship and the Navy unit is required, the FLTCOM OPCONCEN will arrange a specific frequency assignment for coordination purposes. Any required billing will be done per tariff regulations applicable to INMARSAT and HF Public Coast Radio Stations.

U.S. Navy and Air Force HF voice communications nets are dedicated to command and control of military units and air traffic control. These nets will normally not be used for training purposes unless specifically designated by services' operational commander(s) for use by merchant ships as part of a scheduled exercise. However, MERSHIPS may use commercial communications systems (INMARSAT, HF) aboard ship for personnel training and equipment check-out procedures by placing calls to



the FLTCOM OPCONCEN. MERSHIPS will initiate tests by dialing the appropriate FLTCOM OPCONCEN for the ocean area involved. Shipping line owners will fund costs incurred for tests initiated by their merchant ships. The FLTCOM will determine if the test calls should be extended to USN afloat units via the FLTSATCOM interfaces and NCTAMS. The FLTCOM may desire to use HF HICOM for MERSHIPS under Navy control as well as MERSHIPS not under Navy control during Naval Control of Shipping exercises or for test prior to in-chop. Except in crisis situations, MERSHIPS under charter to COMSC will use procedures outlined in other portions of this publication.

n. Frequencies authorized for use by MERSHIPS for emergency communications are listed below:

NAVY			
Control Area	Control Station	Voice Station	SSB Frequencies Call (kHz)
Mediterranean	NCTAMS EURCENT DET LONDON UK		GXH Carrier Freq: 6720
Eastern and Northern Atlantic	NCTAMS EURCENT DET ROTA SP	AOK	Carrier Freq: 11255
Caribbean (Caribbean Emergency Net)	COMNAVACTS Puerto Rico Designated afloat units	CARIB  Any Navy Station this net	Carrier Freq: 7535 kHz Upper Sideband: 7546.5 kHz (24 HR)
	NAVSTA Guantanamo Bay Cuba	NAW	Carrier Freq: 15522 kHz Upper Sideband: 15523.5 kHz (24 HR)
Indian Ocean	NAVCOMTELSTA Diego Garcia	NKW	Carrier Freq: 23315 kHz
Voice Net	Designated afloat units	Any Navy station this net	Upper Sideband: 23316.5 kHz (0200- 1300Z) Carrier Freq: 11205 kHz Upper Sideband: 11206.5 kHz (1300- 0200Z)

## NOTES:

1. NAVCOMTELSTA Iceland guards frequency from 2000-0800Z, NAVCOMTELSTA Puerto Rico from 0001-1345Z.
2. NAVCOMTELSTA Iceland guards frequency from 0800-2000Z.
3. NAVCOMTELSTA Puerto Rico guards frequency from 1345-2359Z.

## EMERGENCY COMMUNICATIONS FREQUENCIES

AIR FORCE			
Control Area	Control Station	Voice Call	SSB (Carrier) Frequencies (Khz)
Southwest Pacific Micronesia	Andersen AFB Guam	"Andersen "	6738 (0200-1200Z) 8967 (24 hr) 11176 (24 hr) 13201 (24 hr) 18002 (2200-0700Z)
Northwest Pacific Sea of Japan	Yokota AB Japan	"Yokota"	4747 (1000-2100Z) 6738 (0900-2400Z) 8967 (24 hr) 11236 (24 hr) 13201 (2100-1000Z) 18002 (0001-0900Z)
Mid Pacific	Hickam AFB Hawaii	"Hickam"	3144 (0600-1700Z) 6738 (0400-0900) 8964 (24 hr) 11179 (24 hr) 13201 (1700-0600Z) 18002 (0001-0900Z)
Northern Pacific	Elmendorf AFB	"Elmendor f"	6738 (24 hr) 8989 (24 hr) 11176 (24 hr) 13201 (24 hr)
Eastern Pacific West Coast CONUS California Mexico	McClellan AFB	"McClella n"	4746 (0400-1600Z) 6738 (0400-1600Z) 8989 (24 hr) 11239 (24 hr) 15031 (1600-0400Z) 18002 (1600-0400Z)
Central America (LANT and PAC) South America (LANT and PAC) Cuba, Hispaniola	Albrook AB Panama	"Albrook"	5710 (0200-1200Z) 6683 (0001-1400Z) 8993 (24 hr) 11176 (24 hr) 15015 (1200-0200Z) 18019 (0900-2400Z)
Northern Atlantic East Coast CONUS, Canada, Caribbean Gulf	McDill AFB Florida	"McDill"	Northern Atlantic 5688 (0001-1400Z) 8989 (24 hr) 11179 (0900-2400Z) 13244 (0900-2400Z)

AIR FORCE			
Control Area	Control Station	Voice Call	SSB (Carrier) Frequencies (Khz)
of Mexico			18019 (0900-2400Z)  Central Atlantic 4746 (0001-0900Z) 6750 (0001-0900Z) 11179 (0900-2400Z) 11246 (24 hr) 13244 (0900-2400Z)  Southern Atlantic 4746 (0001-0900Z) 6750 (0001-0900Z) 8993 (24 hr) 11246 (24 hr) 13244 (0900-2400Z)  Gulf of Mexico 4746 (0001-0900Z) 6750 (0002-0900Z) 8993 (24 hr) 11246 (24 hr)
Northern Atlantic Canada, Greenland	Thule AB	"Thule"	6738 8967 13201 (Slight delay in answering)
Eastern Atlantic Iceland North Sea, Baltic	Croughton AB UK	"Croughton"	3076 (2300-0500Z) 5703 (2100-0800Z) 6750 (24 hr) 9011 (0500-2300Z) 11176 (24 hr) 13214 (0800-2100Z)
Eastern Atlantic Spain, Western Mediterranean, North Africa	Lajes AB Azores	"Lajes"	3081 (2100-1000Z) 4746 (2100-1000Z) 6750 (24 hr) 8967 (24 hr) 11226 (1000-2100Z) 13244 (1000-2100Z)
South Atlantic Cape of Good Hope Western Indian Ocean, Red Sea	Ascension Island Auxiliary AB	"Ascension"	6753 (2000-0800Z) 8993 (24 hr) 11176 (1800-1000Z) 13244 (1000-1800Z) 15015 (08000-2000Z)
Central and Eastern Mediterranean Strait of Hormuz Persian Gulf Northern Red Sea	Incirlik AB Turkey	"Incirlik"	6738 (24 hr) 11176 (24 hr) 13244 (24 hr) 15015 (24 hr)

## AIR FORCE COMMUNICATIONS FREQUENCIES

(SITOR/NBDP)  
ATLANTIC/PACIFIC CALL HF WORKING FREQUENCIES (300HF1B)

This circuit provides common medium and long range radio teletype communications between ship stations (GOVT and NON GOVT) and COMMSTAs for safety and liaison traffic. Calling and working for ship-shore-ship communications will follow the indicated scheduled for freq-guards. Any changes desired by area commanders to meet operational needs will be included in this schedule.

Chesapeake (NMN)  
(1097)\*

Coast Freq	4213.7	6316	8428	12591.5	16819.6	22389.5
	(4212)	(6314.3)	(8426.3)	(12590.8)	(16817.8)	
	(22387.8)					
Ship Freq	4175.7	6266.2	8389.7	12491.7	16698.2	22299.2
	(4174)	(6264.5)	(8388)	(12490)	(16696.5)	
	(22297.5)					
	HN	H24	H24	H24	HJ	HJ

Pt Reyes (NMC)  
(1096)\*

Coast Freq	4215.5	6323.5	8426.0	12600	16815.5	
22386	25380					
	(4213.8)	(6321.8)	(8424.3)	(12598.3)	(16814.8)	
	(22384.3)	(25378.3)				
Ship Freq	4178	6271.7	8386	12497.5	16693	22294
	25202.5					
	(4176.3)	(6270.8)	(8384.3)		(12495.8)	
	(16691.3)	(22292.3)		(25200.8)		
	O/R HN	H24	O/R	HJ	O/R	O/R

Guam (NRV) (Operated remotely from CAMSPAC Pt Reyes)  
(1100)\*

Coast Freq	4215.5	6319.5	8422	12585	16812.5	22382
	(4213.8)	(6317.8)	(8420.3)	(12583.3)		
	(16810.8)		(22380.3)			
Ship Freq	4178	6268.5	8382	12482.5	16689	22290
	(4176.3)	(6266.8)	(8380.3)	(12480.8)		
	(16687.3)		(22288.3)			
	O/R	O/R	HN	H24	H24	HJ

Honolulu (NMO) (Operated remotely from CAMSPAC Pt Reyes)  
(1099)\*

Coast Freq	4212 (4210.3) (16817.8)	6316 (6314.3)	8429.5 (8427.8) (22387.8)	12589 (12587.3)	16819.5 (16817.8)	22389.5 (22387.8)
Ship Freq	4174 (4172.3) (16694.8)	6264.5 (6262.8)	8389.5 (8387.8) (22295.8)	12486.5 (12484.8)	16696.5	22297.5
	O/R	O/R	H24	H24	O/R	HJ

\* Coast station identification number for use with selective calling devices

**Note 1:** The carrier or dial frequency in parenthesis is located 1.7 kHz below the assigned frequency.

**Note 2:** Time definitions

HJ Daytime (2 hours after sunrise until 2 hours before sunset;

local time)

HN Nighttime (2 hours before sunset until 2 hours after sunrise;

local time)

H24 Continuous (24 hours)

#### HF WORKING FREQUENCIES

**THIS PAGE INTENTIONALLY BLANK**

## APPENDIX I

## SAMPLE DRILL PACKAGES

The samples listed here are classified for illustration purposes only, the content is unclassified. The format follows FXP 3 (Rev G) figure 2-1. Italicized areas are to be replaced with appropriate information for the exercise. These are samples only some line items may change as exercise/mission dictates, make changes as appropriate.

Note: Paragraph U (Communications) of the Pre-Ex message can be whatever circuits the strike group chooses to use based on equipment limitations and the nature of the exercise.

## DRILL PACKAGE ALPHA - UHF SECURE/NONSECURE VOICE

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG ALPHA) UHF SECURE/NONSECURE VOICE ACTIVATION. THE CRITERIA FOR MEASURING EFFECTIVENESS OF THE BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE(S). ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. EXERCISE: ACTIVATION OF UHF SECURE/NONSECURE VOICE

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: CO, (PRI) **USS CV/CVN, LHA/LHD (SEC) USS CG**

G. PARTICIPANTS: **Strike Group Units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN.

I. TIME ZONE: ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

U. COMMUNICATIONS: **SIPR CHAT/VOICE COMMS**

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD:

V. INSTRUCTIONS:

V1. ALL UNITS MUST BE PREPARED TO ACTIVATE DESIGNATED CIRCUIT LINE NUMBER UPON REQUEST VIA COMSPOT AS DIRECTED BY THE COMMUNICATION CONTROL SHIP. ROLL CALL ASSIGNMENT WILL BE DESIGNATED BY **the Strike Group Commander**.

V2. OCE WILL CONDUCT ROLL CALL ON VOICE NET **OPTASK COMMS line number**. EACH UNIT WILL INITIATE CALL UP TO THE CCS ADVISING RECEIPT AND READABILITY OF ROLL CALL. ONCE AMPLE CALL UPS ARE RECEIVED, **USS CV/CVN, LHA/LHD** WILL SHIFT TO PLAIN AND COMMUNICATE UTILIZING CALL SIGNS. STRICT USE OF AUTHENTICATION, GINGERBREAD AND EEFI PROCEDURES WILL BE ADHERED TO. **USS CVN/LHA/LHD** WILL

INITIATE NUCO/UN-NUCO TRAFFIC TO ALL PARTICIPANTS.  
ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST THE CAPABILITIES OF  
**CV/CVN, LHA/LHD Strike group** OF ACTIVATING AN UNSCHEDULED UHF  
SECURE/UNSECURE VOICE CIRCUIT. ALL UNITS MUST BE PREPARED TO  
EXECUTE WHEN EXERCISE IS INITIATED.

-----  
- GOAL ACTIVATE UHF SECURE/UNSECURE VOICE.

-----  
- TRANSMIT AND RECEIVE ON UHF VOICE CIRCUIT (SECURE/UNSECURE).  
-----

C4I PKG ALPHA (UHF CIRCUITS) (ACTIVATE UNSKED UHF  
CIRCUIT)  
NMETL/NTA(S)

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

S1. COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARDS:

-----  
S1H. TIME (MINUTES) TO ACTIVATE UHF SECURE/NONSECURE VOICE. (T1)-  
5, (T2) 5-20, (T3) 20-30, (T4)-30  
-----

FXP:

CCC-5-SF SYSTEM CONTROL SECURE/NONSECURE VOICE

CCC-6-SF RADIO-TELEPHONE DRILLS

CCC-34-SF SYSTEM CONTROL - SINGLE AUDIO SYSTEM (SAS) AND BLACK  
AUDIO SYSTEM (BAS)

-----  
- ATTAINABLE GOAL STANDARD REQUIRED IS T2.  
-----

2. (C) CCS WILL GENERATE COMSPOT DETAILING UHF SECURE/NONSECURE  
UPON FINEX. OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF  
EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group CAS: indicate  
IP Address//  
Downgrading instructions in accordance with SECNAV M5510.36 (June  
2006)**



**DRILL PACKAGE BRAVO - HF SECURE/NONSECURE VOICE**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG BRAVO) HF SECURE/NONSECURE VOICE ACTIVATION. THE CRITERIA FOR MEASURING EFFECTIVENESS OF THE BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKTRAPAC CAS(S) SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **strike group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. EXERCISE: ACTIVATION OF HF SECURE/NONSECURE VOICE

B. OSE: **strike group commander**

C. OTC: **strike group commander**

D. OCE: (PRI) **USS CV/CVN, LHA/LHD** (SEC) **USS CG**

G. PARTICIPANTS: **Strike Group Units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN.

I. TIME ZONE: ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

U. COMMUNICATIONS: VOICE COMMS/SIPR CHAT

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD:

V. INSTRUCTIONS:

V1. ALL UNITS MUST BE PREPARED TO ACTIVATE DESIGNATED CIRCUIT LINE NUMBER UPON REQUEST VIA COMSPOT AS DIRECTED BY THE COMMUNICATION CONTROL SHIP (CCS). ROLL CALL ASSIGNMENT WILL BE DESIGNATED BY OCE. HF PREDICTION AND PROPAGATION WILL BE DETERMINED PRIOR TO EXECUTION OF DRILL. CCS WILL GENERATE HF PREDICTION MESSAGE TO SUPPORT THIS EXERCISE.

V2. OCE WILL CONDUCT ROLL CALL ON PRIMARY CIRCUIT **OPTASK COMMS line number**. EACH UNIT WILL INITIATE CALL UP TO THE CCS ADVISING RECEIPT AND READABILITY OF ROLL CALL. ONCE AMPLE CALL UPS ARE RECEIVED, GINGERBREAD PROCEDURES WILL BE ADHERED TO. **USS CV/CVN, LHA/LHD** WILL INITIATE NUCO/UN-NUCO TRAFFIC TO ALL PARTICIPANTS.

ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST THE CAPABILITIES OF **CV/CVN, LHA/LHD Strike group** OF ACTIVATING AN UNSCHEDULED HF SECURE/

UNSECURE VOICE CIRCUIT. ALL UNITS MUST BE PREPARED TO EXECUTE WHEN EXERCISE IS INITIATED.

-----  
- GOAL ACTIVATE HF SECURE/UNSECURE VOICE.  
-----

-----  
- TRANSMIT AND RECEIVE ON HF VOICE CIRCUIT (SECURE/UNSECURE).  
-----

C4I PKG BRAVO (HF CIRCUITS) (ACTIVATE UNSKED HF CIRCUIT)

NMETL/NTA(S)

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

S1. COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARDS:

-----  
S1H. TIME (MINUTES) TO ACTIVATE HF TTY CIRCUIT.  
T1<= 5, T2>5-20, T3>20-30, T4>30  
-----

FXP:

CCC-5-SF SYSTEM CONTROL SECURE/NONSECURE VOICE  
CCC-6-SF RADIO-TELEPHONE DRILLS  
CCC-34-SF SYSTEM CONTROL - SINGLE AUDIO SYSTEM (SAS) AND BLACK  
AUDIO SYSTEM (BAS)  
-----

- ATTAINABLE GOAL STANDARD REQUIRED IS T2.  
-----

2. (C) CCS WILL GENERATE COMSPOT DETAILING HF SECURE/NONSECURE  
UPON FINEX. OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF  
EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS SITE:

**Indicate IP Address.//**

**Downgrading instructions in accordance with SECNAV M5510.36 (June  
2006)**

**DRILL PACKAGE CHARLIE - EHF PERFORMANCE AND CIRCUIT ACTIVATION**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG CHARLIE) FOR EHF EXTERNAL COMMUNICATIONS AND MEASURES OF EFFECTIVENESS GRADING CRITERIA. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE(S). ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. PROVIDE EXTERNAL EHF COMMUNICATIONS FOT LDR, MDR, AND NECC.

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: (PRI) **USS CV/CVN, LHA/LHD** (SEC) **USS CG**

G. PARTICIPANTS: **Strike Group Units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN IAW REF B SCHEDULE OF EVENTS (SOE).

I. TIME ZONE: ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

U. COMMUNICATIONS: PRIMARY WARFARE COMMANDERS VOICE AND CHATCIRCUITS AS DESIGNATED IN STRIKE GROUP EFFECTIVE OPTASK COMMS ISO TRANSLANT.

U. COMMUNICATIONS: **SIPR CHAT/VOICE COMMS**

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD:

V. INSTRUCTIONS:

V1. OCE WILL ANNOUNCE THE ACTIVATION OF NETS OR REQUEST PERFORMANCE STATUS UPON NOTICE. ALL UNITS MUST BE PREPARED TO EXECUTE WHEN EXERCISE IS INITIATED.

-----  
ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST **CV/CVN, LHA/LHD** STRIKE GROUP'S ABILITY TO CONDUCT EHF FOT PERFORMANCE AND CIRCUIT ACTIVATIONS TO MEET NMETL/NTA STANDARDS ISO COMPTUEX OBJECTIVES.  
-----

- MAINTAIN ATTAINABLE GOAL STANDARD REQUIRED OF T2.  
-----

- PROVIDED BELOW ARE THE LISTED NMETL/NTA OBJECTIVES WHICH WILL BE OBSERVED.  
-----

C4I PKG CHARLIE (EHF LDR/MDR/FOT/NECC SYSTEM PERFORM EXERCISE)  
(PERFORM VARIOUS EHF SYSTEM CHECKS)

NMELT/NTA(S)  
-----

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS EHF  
LDR/MDR/FOT/NECC  
-----

--

DEMONSTRATE ABILITY TO INTERPRET RF PERFORMANCE SCREEN AND CONDUCT SATELLITE LOOP TEST (SLT). T1=YES, T2=N/A, T3=N/A, T4=NO.

- WHEN DIRECTED BY NECOS ALL UNITS WILL SEND COMSPOT DETAILING THE RF PERFORMANCE SCREEN.

-----  
-  
(NECC)

TIME IN (MINUTES) TO LOAD THE CORRECT NECC COMM CONFIGURATION FOR CURRENT AOR. T1=<15, T2=15-30, T3=30-45, T4=>45.

- OCE WILL PROVIDE STATUS ON ALL UNITS REACHABLE VIA NECC.

- OCE WILL CONDUCT OTO WITH ALL REACHABLE UNITS.

- OCE WILL HANOVER NECOS VIA NECC.

-----  
---  
TERMINAL FAULT STATUS

TIME IN (MINUTES) TO PERFORM AUTOMATIC TEST SEQUENCE (ATS) TO ENSURE NO FAULTS ARE PRESENT. T1=<5, T2=6-7, T3=8-9, T4=>9.

- ENSURE A QUALIFIED EHF TECH IS PRESENT WITH THE EHF OPERATOR WHEN CONDUCTING ANY PERFORMANCE TESTING.

- NECOS WILL DESIGNATE WHEN EACH UNIT WILL CONDUCT ATS.

- UPON COMPLETION PROVIDE STATUS OF ATS FAULTS VIA COMSPOT.

-----  
---  
TIME IN (MINUTES) TO DEMONSTRATE JOINING A BEAM MANAGED (BM) NET.

T1=<5, T2=6-10, T3=11-15, T4=>15.

- NECOS WILL DIRECT ALL UNITS TO EXIT ALL LDR AND MDR NETS LESS ADNS DUAL SIMPLEX NETS.

- NECOS WILL ORDER THE ACTIVATION OF DESIGNATED NET FOR ALL UNITS.

-----  
FXP:  
CCC-26-SF EXTREMELY HIGH FREQUENCY SATELLITE COMMUNICATIONS  
-----

2.) OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS II: **indicate IP address.**//  
**Downgrading instructions in accordance with SECNAV M5510.36 (June 2006)**

**DRILL PACKAGE CHARLIE ONE - EHF POINT TO POINT (PTP)**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG CHARLIE-ONE) FOR EHF POINT TO POINT COMMUNICATIONS AND MEASURES OF EFFECTIVENESS GRADING CRITERIA. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKGORTRAPAC CAS SITE(S). ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

- A. EXERCISE: EHF POINT TO POINT ACTIVATION
- B. OSE: **Strike Group Commander**
- C. OTC: **Strike Group Commander**
- D. OCE: (PRI) **USS CV/CVN, LHA/LHD** (SEC) **USS CG**
- G. PARTICIPANTS: **Strike Group Units**
- I. TIME ZONE: ZULU
- J. COMEX: IAW SOE (NO NOTICE)
- JJ. FINEX: IAW SOE
- N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED
- U. COMMUNICATIONS: **SIPR CHAT/VOICE COMMS**
  - A. COORDINATION CIRCUITS:
    - 1. PRI COORD:
    - 2. SEC COORD:

V. INSTRUCTIONS:

V1. ALL UNITS BE PREPARED TO ACTIVATE EHF PTP ON CALL AT A MOMENTS NOTICE IAW WITH COMEX/FINEX TIME PERIOD INDICATED. CCS WILL DESIGNATE TIME TO ACTIVE EHF PTP VIA IMMEDIATE COMSPOT. CCS WILL INDICATE THE ORDER OF SHIPS FOR THE CALL IN THE COMSPOT.

V2. ALL UNITS MUST HAVE USKAT B5693 AND USKAT B5697 TO BE PREPARED TO CONDUCT PTP AND CROSSLINK WITH UNITS IN **C2F, C6F, C5F, AND C7F**. ENSURE UNIT DIRECTORY TERMINAL ID(S) ARE AVAILABLE AT ALL TIMES. ALL PARTICIPANTS MUST BE PREPARED TO ACTIVATE PTP UPON NOTICE. ALL UNITS MUST BE PREPARED TO EXECUTE WHEN EXERCISE IS INITIATED.

-----

ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST **CV/CVN, LHA/LHD's** STRIKE GROUP ABILITY TO RECEIVE AN EHF PTP AND MEET THE T1 ATTAINABLE GOAL.

-----

C4I PKG CHARLIE ONE (EHF P-T-P)

NMETL/NTA(S)

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS EHF LDR/MDR/FOT/NECC

S1. COMMUNICATIONS CONTROL SHIP'S EFFECTIVENESS STANDARDS

TIME IN (MINUTES) TO ESTABLISH AN EHF PTP VOICE CIRCUIT WITH STRIKE GROUP UNITS.

(T1) -5, (T2) 6-15, (T3) 16-30, (T4) 30.

-----  
FXP:

CCC-26-SF EXTREMELY HIGH FREQUENCY SATELLITE COMMUNICATIONS  
-----

2. (C) OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF  
EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS II:  
**indicate IP address.//**

**Downgrading instructions in accordance with SECNAV M5510.36 (June  
2006)**

**DRILL PACKAGE DELTA - BATTLE FORCE EMAIL NETWORK ACTIVATION**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG DELTA) BATTLE FORCE EMAIL NETWORK ACTIVATION AND THE CRITERIA FOR MEASURING EFFECTIVENESS OF THE BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE(S). ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **strike group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. EXERCISE: BATTLE FORCE EMAIL ACTIVATION IAW NTA5.1.1.2 S1I

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: (PRI) USS **CV/CVN, LHA/LHD** (SEC) USS **CG**

G. PARTICIPANTS: **Strike Group Units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN.

I. TIME ZONE: ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

U. COMMUNICATIONS: **SIPR CHAT/VOICE COMMS**

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD:

V. INSTRUCTIONS:

V1. ALL UNITS BE PREPARED TO ACTIVATE DESIGNATED CIRCUIT LINE NUMBER UPON REQUEST. HF PREDICTION AND PROPAGATION WILL BE DETERMINED PRIOR TO EXECUTION OF DRILL.

V2. VERIFY BFEM 66 GATEWAY SERVER IS ACTIVE (BOTH HF MESSENGER APPLICATIONS - SMS AND HF DELIVERY AGENT).

V3. VERIFY MICROSOFT EXCHANGE SERVER IS RUNNING PROPERLY WITH GATEWAY SERVER.

V4. VERIFY USER ACCOUNTS/PASSWORDS ARE BUILT.

V5. VERIFY PROPER SETUP OF RF EQUIPMENT. SYSTEM MUST BE OPERATING PROPERLY PRIOR TO EXECUTION OF DRILL.

V6. CCS IS REQUIRED TO TRANSMIT THREE EMAIL MESSAGES ADDRESSED TO ALL PARTICIPANTS. ALT CCS WILL TRANSMIT THREE EMAIL MESSAGES TO ALL PARTICIPANTS. ALL PARTICIPANTS ARE TO QSL ALL THREE MESSAGES UTILIZING BATTLEFORCE EMAIL, AND SEND A COMSPOT TO CCS AND **Strike Group Commander**.

V7. IN CASE OF EQUIPMENT PROBLEMS, PASS RESULTS OF DRILL (I.E. PROBLEMS, TROUBLESHOOTING EFFORTS) TO OCE VIA **Usually SIPR CHAT or Radio email address**. UNITS ARE ENCOURAGED TO CONTINUE TROUBLESHOOTING AFTER DRILL IS COMPLETE. CONTACT CCS FOR SME ASSISTANCE IF REQUIRED. TROUBLESHOOTING VIA SIPR CHAT WITH ALL UNITS IS HIGHLY ENCOURAGED. ALL UNITS MUST BE PREPARED TO EXECUTE WHEN EXERCISE IS INITIATED.

- 
- GOAL IS TO MAINTAIN BFEM OPERATIONS AND ACTIVATE CIRCUIT USING NMTEL/NTA NTA5.1.1.2 S1I.

STANDARDS FOR ACTIVATION ISAS FOLLOWS:

-----  
T1 0-5 MINS - T2 5-20 MINS - T3 20-30 MINS - T4 30 MINS  
-----

ATTAINABLE GOAL STANDARD REQUIRED IS T2.  
-----

2). OCE WILL DEBRIEF VIA **COMM COORD CHAT**. OCE WILL PROVIDE GRADE  
STANDARDS AND MEASURES OF EFFECTIVENESS RESULTS WILL BE POSTED  
VIA **Strike Group** CAS II: **indicate IP address.**//  
**Downgrading instructions in accordance with SECNAV M5510.36 (June  
2006)**



**DRILL PACKAGE ECHO - FREQUENCY SHIFT AND KICK PROCEDURES**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG ECHO) FOR WARFARE CMDRS FREQUENCY SHIFT AND KICKS. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT AND COMSTRKFORTRAPAC CAS SITE(S). ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. WARFARE COMMANDER FREQUENCY SHIFTS AND KICKS.

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: (PRI) **USS CV/CVN, LHA/LHD** (SEC) **USS CG**

G. PARTICIPANTS: **Strike group units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN IAW REF B (MTO).

I. TIME ZONE: ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

U. COMMUNICATIONS: PRIMARY WARFARE COMMANDERS VOICE AND CHAT CIRCUITS AS DESIGNATED IN **Strike Group's** EFFECTIVE OPTASK COMMS ISO **exercise/evolution**.

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD:

V. INSTRUCTIONS:

V1. EACH WARFARE COMMANDER WILL BE RESPONSIBLE FOR INITIATING FREQUENCY SHIFTS OR KICKS AT LEAST TWICE DAILY UTILIZING ASSIGNED CIRCUITS AND FREQUENCIES PROVIDED VIA THE EFFECTIVE OPTASK COMMS.

V2. ALL IT(S) IN MAINCOMM WILL BE READY TO ASSIST INDIVIDUAL WARFARE CMDRS WITH DETERMINING BEST COURSE OF ACTION AND EXECUTION WHEN SHIFTING FREQUENCIES BASED ON EQUIPMENT STATUS AND AVAILABILITY OF RESOURCES.

-----  
 ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST **strike group** ABILITY TO SHIFT FREQUENCIES AND MEET NMETL/NTA STANDARDS ISO **exercise/evolution** OBJECTIVES.  
 -----

- GOAL WILL BE TO SHIFT FREQUENCIES/CIRCUITS AS DIRECTED BY WARFARE CMDRS.  
 -----

- MAINTAIN ATTAINABLE GOAL STANDARD REQUIRED OF T2.  
 -----

- GOAL WILL BE TO MAINTAIN ASSIGNED AND GUARDED WARFARE CMDR NETS. ALL CIRCUITS MUST BE ACTIVATED AS DIRECTED ISO EXECUTING C4I EXERCISE EVENT.  
 -----

- PROVIDED BELOW ARE THE NMETL/NTA OBJECTIVES WHICH WILL BE OBSERVED.  
 -----

C4I PKG ECHO (KICK DRILL) (WARFARE CMDR CIRCUITS SHIFTS/KICK)

NMETL/NTA(S)

-----  
NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

S1.- COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARDS

S4.- WARFARE COMMANDER CIRCUIT SHIFTS (KICK)  
(INCLUDES VOICE OR CHAT AS DESIGNATED VIA OPTASK COMMS)

S4A.- TIME (MINUTES) TO SHIFT AND RESTORE COMMUNICATIONS ON  
SCC PRIMARY WARFARE NET FROM AN ESTABLISHED NET TO A DESIGNATED  
ALTERNATE NET (IAW COMPLAN) AND COMPLETE ROLL CALL WITH  
APPROPRIATE STRIKE GROUP UNITS WHEN DIRECTED.

(T1)-5, (T2) 5-10, (T3) 10-15, (T4)-15

-----  
S4B. TIME (MINUTES) TO SHIFT AND RESTORE COMMUNICATIONS ON IWC  
PRIMARY WARFARE NET FROM AN ESTABLISHED NET TO A DESIGNATED  
ALTERNATE NET (IAW COMPLAN) AND COMPLETE ROLL CALL WITH  
APPROPRIATE STIKE GROUP UNITS WHEN DIRECTED.

(T1)-5, (T2) 5-10, (T3) 10-15, (T4)-15

-----  
S4C. TIME (MINUTES) TO SHIFT AND RESTORE COMMUNICATIONS ON ADC  
PRIMARY WARFARE NET FROM AN ESTABLISHED NET TO A DESIGNATED  
ALTERNATE NET (IAW COMPLAN) AND COMPLETE ROLL CALL WITH  
APPROPRIATE STRIKE GROUP UNITS WHEN DIRECTED.

(T1)-5, (T2) 5-10, (T3) 10-15, (T4)-15

-----  
S4E. TIME (MINUTES) TO SHIFT AND RESTORE COMMUNICATIONS ON STRIKE  
WARFARE COMMANDER'S PRIMARY WARFARE NET FROM AN ESTABLISHED NET  
TO A DESIGNATED ALTERNATE NET (IAW COMPLAN) AND COMPLETE ROLL  
CALL WITH APPROPRIATE STRIKE GROUP UNITS WHEN DIRECTED.

(T1)-5, (T2) 5-10, (T3)> 10-15, (T4)-15

-----  
S4F. TIME (MINUTES) TO SHIFT AND RESTORE STRIKE GROUP CHAT  
COMMUNICATIONS ON SECONDARY CHAT SERVER (IAW OPTASK COMMS/OPTASK  
IM) WHEN DIRECTED.

(T1)-5, (T2) 5-10, (T3)> 10-15, (T4)-15

-----  
S3. STRIKE GROUP COMMAND AND REPORTING NETS EFFECTIVENESS

-----  
- CHAT ROOM SHIFTS

S3A. ABILITY OF SEA COMBAT COMMANDER COMMAND AND REPORTING NET  
SUPPORT SCC COMMUNICATIONS WITH ALL UNITS DIRECTED TO GUARD THE  
CIRCUIT/DESIGNATED CHAT ROOM AS PER OPTASK COMMS (PERCENT AVERAGE  
DAILY AVAILABILITY).

(T1)-98, (T2) 98-95, (T3) 95-90, (T4)-90

S3B. ABILITY OF IWC COMMAND AND REPORTING NET TO SUPPORT IWC COMMUNICATIONS WITH ALL UNITS DIRECTED TO GUARD THE CIRCUIT/DESIGNATED CHAT ROOM AS PER OPTASK COMMS (PERCENT AVERAGE DAILY AVAILABILITY).

(T1)-98, (T2) 98-95, (T3) 95-90, (T4)-90

S3C. ABILITY OF ADC COMMAND AND REPORTING NET TO SUPPORT ADC COMMUNICATIONS WITH ALL UNITS DIRECTED TO GUARD THE CIRCUIT/DESIGNATED CHAT ROOM AS PER OPTASK COMMS (PERCENT AVERAGE DAILY AVAILABILITY).

(T1)-98, (T2) 98-95, (T3) 95-90, (T4) 90

S3E. ABILITY OF STRIKE COMMAND AND REPORTING NET TO SUPPORT STRIKE COMMUNICATIONS WITH ALL UNITS DIRECTED TO GUARD THE CIRCUIT/DESIGNATED CHAT ROOM AS PER OPTASK COMMS (PERCENT AVERAGE DAILY AVAILABILITY).

(T1)- 98, (T2) 98-95, (T3) 95-90, (T4) 90

S3F. ABILITY OF SELECTED (CHAT, ALTERNATE CIRCUITS AS DIRECTED) STRIKE GROUP COMMAND AND REPORTING NETS TO SUPPORT STRIKE GROUP COMMUNICATIONS WITH ALL UNITS DIRECTED TO GUARD THE CIRCUIT/DESIGNATED CHAT ROOM AS PER OPTASK COMMS (PERCENT AVERAGE DAILY AVAILABILITY).

(T1)- 98, (T2) 98-95, (T3) 95-90, (T4) 90

-----  
- NOTE WARFARE COMMANDER WILL INITIATE AND EXECUTE FREQUENCY/SHIFT. THIS ALSO INCLUDES MAINTAINING ROLL AS WELL.

- CONNECTIVITY OF ALL DESIGNATED CIRCUITS EITHER VOICE OR CHAT WILL BE MONITORED BY BOTH CCSG12 AND INDIVIDUAL WARFARE CMDRS.

-TOTAL TIME OF CIRCUITS ACTIVE WILL BE RECORDED AND PROVIDED AT THE END OF RADIO DAY.

- CWC/IWC/ADC/SCC/STWC WARFARE CMDRS WILL THEN CONDUCT ROLL CALL IMMEDIATELY AFTER SHIFT IS EXECUTED.

- HF, UHF, AND SATCOM WILL BE UTILIZED DURING THE EXERCISE.  
-----

FXP's:

CCC-5-SF SECURE/NON-SECURE VOICE SYSTEMS

CCC-6-SF RADIO TELEPHONE DRILLS

CCC-24-SF NARROWBAND/WIDEBAND SATELLITE COMMUNICATION SYSTEMS

2.) OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS II:

**indicate IP address.//**

**Downgrading instructions in accordance with SECNAV M5510.36 (June**

2006)

**DRILL PACKAGE ECHO ONE - WARFARE COMMANDERS ROLL CALL**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG ECHO ONE) FOR WARFARE CMDRS 24 HOUR ROLL CALLS. MEASURES OF EFFECTIVENESS AND GRADING CRITERIA. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. WARFARE COMMANDER(S) PRIMARY GUARDED CIRCUIT 24 HOUR ROLL CALLS.

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: **USS CV/CVN, LHA/LHD (SEC) USS CG**

G. PARTICIPANTS: **Strike group units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN IAW REF B SCHEDULE OF EVENTS (SOE).

I. TIME ZONE: ALL TIMES ARE ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

U. COMMUNICATIONS: PRIMARY WARFARE COMMANDERS VOICE AND CHAT CIRCUITS AS DESIGNATED IN **strike group** EFFECTIVE OPTASK COMMS ISO **exercise/evolution**.

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD:

V. INSTRUCTIONS:

V.1 EACH WARFARE COMMANDER WILL BE RESPONSIBLE FOR INITIATING FREQUENCY SHIFTS OR KICKS AT LEAST TWICE DAILY UTILIZING ASSIGNED CIRCUITS AND FREQUENCIES PROVIDED VIA THE EFFECTIVE OPTASK COMMS.

V.2 ALL IT(S) IN MAINCOMM WILL BE READY TO ASSIST INDIVIDUAL WARFARE CMDRS WITH DETERMINING BEST COURSE OF ACTION AND EXECUTION WHEN SHIFTING FREQUENCIES BASED ON EQUIPMENT STATUS AND AVAILABILITY OF RESOURCES.

-----  
 ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST **strike group** ABILITY TO SHIFT FREQUENCIES AND MEET NMETL/NTA STANDARDS ISO **exercise/evolution** OBJECTIVES.  
 -----

- GOAL WILL BE TO SHIFT FREQUENCIES/CIRCUITS AS DIRECTED BY WARFARE CMDRS.  
 -----

- MAINTAIN ATTAINABLE GOAL STANDARD REQUIRED OF T2.  
 -----

- GOAL WILL BE TO MAINTAIN ASSIGNED AND GUARDED WARFARE CMDR NETS. ALL CIRCUITS MUST BE ACTIVATED AS DIRECTED ISO EXECUTING C4I EXERCISE EVENT.

-----  
- PROVIDED BELOW ARE LISTED THE NMETL/NTA OBJECTIVES WHICH WILL  
BE OBSERVED.  
-----

C4I PKG ECHO ONE (WARFARE COMMANDERS ROLL CALLS)

NMETL/NTA(S)  
-----

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

S1.- COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARDS  
NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

S3A. ABILITY OF SEA COMBAT COMMANDER COMMAND AND REPORTING NET  
SUPPORT SCC COMMUNICATIONS TO MAINTAIN 24 HOUR ROLL CALL  
ACCOUNTABILITY ON DESIGNATED CIRCUIT(S) WITH ALL UNITS (PERCENT  
AVERAGE DAILY AVAILABILITY) .

(T1)-98, (T2) 98-95, (T3) 95-90, (T4)-90

S3B. ABILITY OF IWC COMMAND AND REPORTING NET TO SUPPORT IWC  
COMMUNICATIONS TO MAINTAIN 24 HOUR ROLL CALL ACCOUNTABILITY ON  
DESIGNATED CIRCUIT(S) WITH ALL UNITS (PERCENT AVERAGE DAILY  
AVAILABILITY) .

(T1)-98, (T2) 98-95, (T3) 95-90, (T4)-90

S3C. ABILITY OF ADC COMMAND AND REPORTING NET TO SUPPORT ADC  
COMMUNICATIONS TO MAINTAIN 24 HOUR ROLL CALL ACCOUNTABILITY ON  
DESIGNATED CIRCUIT(S) WITH ALL UNITS (PERCENT AVERAGE DAILY  
AVAILABILITY) .

(T1)-98, (T2) 98-95, (T3) 95-90, (T4)-90

S3E. ABILITY OF STRIKE COMMAND AND REPORTING NET TO SUPPORT  
STRIKE COMMUNICATIONS TO MAINTAIN 24 HOUR ROLL CALL  
ACCOUNTABILITY ON DESIGNATED CIRCUIT(S) WITH ALL UNITS (PERCENT  
AVERAGE DAILY AVAILABILITY) .

(T1)-98, (T2) 98-95, (T3) 95-90, (T4)-90  
-----

- NOTE WARFARE COMMANDERS WILL CONDUCT THE FOLLOWING:
- INITIATE AND EXECUTE ROLL CALLS.
- DESIGNATE ROLL CALLS AND CONDUCT DAILY THROUGHOUT THE 24 HOUR PERIOD.
- MONITOR CONNECTIVITY PERCENTAGE OF ALL DESIGNATED VOICE CIRCUITS.
- PROVIDE TOTAL TIME CIRCUITS ACTIVE AT THE END OF RADIO DAY VIA

CHAT AND OPREP-5 FEEDER.

-----  
FXP's:

CCC-5-SF SECURE/NON-SECURE VOICE SYSTEMS

CCC-6-SF RADIO TELEPHONE DRILLS

CCC-24-SF NARROWBAND/WIDEBAND SATELLITE COMMUNICATION SYSTEMS  
-----

2.) OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF  
EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS II:

**indicate IP address.//**

**Downgrading instructions in accordance with SECNAV M5510.36 (June  
2006)**

**DRILL PACKAGE FOXTROT - ATO AND DIMS TRANSFER**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG FOXTROT) FOR ATO/DIMS TRANSMISSION. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. EXERCISE: ATO AND DIMS TRANSMISSION

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: **USS CV/CVN, LHA/LHD (SEC) USS CG**

G. PARTICIPANTS: **Strike group units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN IAW REF B (MTO).

I. TIME ZONE: ALL TIMES ARE ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

U. COMMUNICATIONS: ATO SEND AND RECEIVE DISTRO PATHS ARE SIPR EMAIL, BF EMAIL, EHF (MDR) ATO TTY, SIPRNET CAS SITE, CNFC CAS, SATCOM CSG TTY, AND HF TTY. THE COMMUNICATIONS CONTROL SHIP (CCS) WILL DESIGNATE DAILY PATHS FOR ATO/DIMS TRANSMISSION VIA COMSPOT IAW SCHEME OF MANEUVER AND SOE.

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD:

V. INSTRUCTIONS:

V1. CCS MAINCOMM WILL TRANSMIT A DAILY COMSPOT INDICATING ATO OR DIMS PATHS TO BE UTILIZED DURING EXERCISE NLT 1300 LOCAL TO ALL **Strike Group** PARTICIPANTS.

THE FOLLOWING ARE METHODS FOR TRANSMISSION:

A. **Strike Group** CAS (**IP ADDRESS**)

B. SIPRNET EMAIL (RADIO@**CVN/LHA Strike Group ##**.NAVY.SMIL.MIL/RADIO@**CCS**.NAVY.SMIL.MIL) OR (RADIO**ALTCCS**.NAVY.SMIL.MIL)

C. CENTRIXS OR NTIDS AS ASSIGNED WHEN DIRECTED

D. HF BFEM AS INDICATED VIA COMSPOT.

E. HF TTY

F. DAMA TTY (**LINE NUMBER**)

G. EHF (MDR) ATO TTY (**LINE NUMBER**)

H. NAVMACS II SMTP (SHIP TO SHIP)

V.2. ATO REPORTING RESPONSIBILITIES:

- ALL UNITS WILL PROVIDE TIME OF RECEIPT VIA COMSPOT FOR ALL PATHS AS DIRECTED BY CCS. IF UNABLE TO RECEIVE/RELAY ATO OR DIMS SEND COMSPOT IMMEDIATELY TO NOTIFY CCS.

- CCS WILL DESIGNATE A UNIT TO PROVIDE RELAY ASSISTANCE OF ANY ATO/DIMS TO OTHERS TO MEET NTA OR NMETL/NTA STANDARD.

B. **CV/CVN, LHA/LHD and strike group commander** WILL MAINTAIN LOGGING TO TRACK TRANSMISSION TIME, AND TIME OF RECEIPT BY EACH UNIT.

ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST **Strike Group** ATO



TRANSMISSION, DELIVERY, AND RECEIPT CAPABILITIES. ALL UNITS MUST BE PREPARED TO EXECUTE WHEN EXERCISE IS INITIATED.

-----  
- GOAL IS TO DELIVER A SOLID COPY OF THE ATO/DIMS TO ALL UNITS.  
-----

- GOAL IS TO MAINTAIN ALL ATO PATHS AND ENSURE ALL SYSTEMS ARE OPERATIONAL. ALL CIRCUITS MUST BE ACTIVE PRIOR TO COMEX ISO EXECUTING C4I EXERCISE EVENT.  
-----

C4I PKG FOXTROT (ATO SND/RCV DATA) (ATO ALL PATHS SND/RCV)  
NMETL/NTA(S)/FXP  
-----

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

S1. COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARDS:  
-----

S1F. PERCENT OF EVERY APPLICABLE COMM PATH USED TO SEND/RECEIVE DATA (SELECTED MESSAGE I.E. ATO, DIMS ETC...).

(T1)-98, (T2) 98-90, (T3) 90-80, (T4) 80  
-----

S1G. AVERAGE TIME (HOURS) TO DISSEMINATE (SELECTED MESSAGE I.E. ATO, DIMS ETC...) TO ALL STRIKE GROUP UNITS.

(T1)-1.5, (T2) 1.5 - 2, (T3) 2 - 3, (T4) 3  
-----

- AVG TIME IN MINUTES WILL BE EVALUATED TO DISSEMINATE ATO TO ALL SG UNITS.  
-----

- ATTAINABLE GOAL STANDARD REQUIRED IS T2.  
-----

FXP's:

CCC-4-SF SYSTEM CONTROL - SHIP TERMINATION FOR B, C, D AND G SYSTEMS

CCC-26-SF EXTREMELY HIGH FREQUENCY SATELLITE COMMUNICATIONS

2.) CCS WILL GENERATE AN ATO STATUS REPORT VIA COMSPOT UPON FINEX. OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS II: **indicate IP address.//Downgrading instructions in accordance with SECNAV M5510.36 (June 2006)**

**DRILL PACKAGE GOLF - VTC ACTIVATION**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG GOLF) GENSER, JWICS, AND TANDBERG VTC. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **strike group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. PROVIDE GENSER VTC.

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: **USS CV/CVN, LHA/LHD (SEC) USS CG**

G. PARTICIPANTS: **Strike group units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN IAW REF B SCHEDULE OF EVENTS (SOE).

I. TIME ZONE: ALL TIMES ARE LOCAL

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

U. COMMUNICATIONS: SIPR CHAT/VOICE COMMS

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD:

V. INSTRUCTIONS:

V1. ALL UNITS MUST BE PREPARED TO ACTIVATE DESIGNATED CIRCUIT LINE NUMBER UPON REQUEST VIA COMSPOT AS DIRECTED BY THE COMMUNICATION CONTROL SHIP. UNITS MUST BE PREPARED TO EXECUTE WHEN EXERCISE IS INITIATED.

V2. DESIGNATED UNITS WILL CONDUCT BRIDGE CHECK AS DIRECTED. ALL UNITS WILL OBTAIN AUDIO/VISUAL CHECK WITH BRIDGE.

-----  
 ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST STRIKE GROUP ABILITY TO CONDUCT GENSER VTC TO MEET NMETL/NTA STANDARDS ISO **exercise/evolution** OBJECTIVES.  
 -----

- MAINTAIN ATTAINABLE GOAL STANDARD REQUIRED OF T2.  
 -----

- PRIOR COORDINATION REQUIRED WITH DISTANT END USER(S)  
 -----

- NOT TO INTERFERE WITH NORMAL VTC WINDOW PREVIOUSLY SCHEDULED  
 -----

- PROVIDED BELOW ARE THE LISTED NMETL/NTA OBJECTIVES WHICH WILL BE OBSERVED.  
 -----

C4I PKG GOLF (GENSER VTC/JWICS/TANDBERG VTC)  
 (ACTIVATE UNSKED VTC GENSER)

NMETL/NTA(S)

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

-----  
DEMONSTRATE ABILITY TO PERFORM VTC.

(T1) = YES, (T2) = N/A, (T3) = N/A, (T4) = NO.

- WHEN DIRECTED BY CCS ALL UNITS WILL INITIATE AUDIO/VIDEO CHECK.  
-----

TIME IN (MINUTES) TO DEMONSTRATE VTC.

(T1) < 5, (T2) 6-10, (T3) 11-15, (T4) > 15.

- CCS WILL DIRECT ALL UNITS TO EXIT VTC AUDIO/VIDEO CHECK.

- CCS WILL ORDER THE ACTIVATION OF DESIGNATED NET FOR ALL UNITS.  
-----

CCC-25-SF SUPER HIGH FREQUENCY SATELLITE COMMUNICATIONS  
-----

2. OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS II: **indicate IP address.**//

**Downgrading instructions in accordance with SECNAV M5510.36 (June 2006)**

**DRILL PACKAGE HOTEL - HF TTY ACTIVATION**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG HOTEL) HF TTY ACTIVATION AND THE CRITERIA FOR MEASURING EFFECTIVENESS OF THE BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS. UNITS MUST BE PREPARED TO EXECUTE WHEN EXERCISE IS INITIATED.

A. EXERCISE: HF TTY ACTIVATION

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: **USS CV/CVN, LHA/LHD (SEC) USS CG**

G. PARTICIPANTS: **Strike group units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN.

I. TIME ZONE: ALL TIMES ARE ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

U. COMMUNICATIONS: SIPR CHAT/VOICE COMMS/TELETYPE RELAY

A. COORDINATION CIRCUITS:

1. PRI PRI COORD:

2. SEC COORD:

3. TTY NET: TELETYPE CIRCUIT DIRECTED

V. INSTRUCTIONS:

V.1. ALL UNITS MUST BE PREPARED TO ACTIVATE DESIGNATED CIRCUIT LINE NUMBER UPON REQUEST VIA COMSPOT AS DIRECTED BY THE COMMUNICATION CONTROL SHIP. HF PREDICTION AND PROPAGATION WILL BE DETERMINED PRIOR TO EXECUTION OF DRILL. CCS WILL GENERATE HF PREDICTION MESSAGE TO SUPPORT THIS EXERCISE.

V2. UNIT DESIGNATED WILL GENERATE A QUICK BROWN FOX TEST TO ALL PARTICIPANTS. EACH UNIT WILL INITIATE CALL UP TO THE CONTROL SHIP ADVISING RECEIPT AND READABILITY OF THE TEST. ONCE AMPLE CALL UPS ARE RECEIVED, CCS WILL TRANSMIT 5 MESSAGES IN A STRING AND UPON COMPLETION RECIPIENT WILL PROVIDE TIME FO RECEIPT VIA COMSPOT.

V3. ALL PARTICIPANTS WILL PROVIDE A PRINT ACCEPTABILITY (ZBZ 1-5) REPORT VIA **Strike Group** COMM COORD. CCS WILL PROVIDE A QRY LIST INDICATING EACH UNITS TURN TO TRANSMIT.

V4. ALL PARTICIPANTS MUST PAY SPECIAL ATTENTION TO THE ZBO AND BE PREPARED TO RESPOND TO ACTION MESSAGES AS THEY APPLY.

ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST **CV/CVN, LHA/LHD** STRIKE GROUP ATO TRANSMISSION, DELIVERY, AND RECEIPT CAPABILITIES.

-----  
- GOAL ACTIVATE ENTSG WORKING HF TTY.  
-----

- TRANSMIT AND RECEIVE MESSAGE TRAFFIC VIA ENTSG COMM COORD HF TTY.  
-----

C4I PKG HOTEL (HF CIRCUITS) (ACTIVATE UNSKED HF CIRCUIT)  
NMETL/NTA(S)/FXP

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

(S1.) COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARDS:  
-----

(S1H.) TIME (MINUTES) TO ACTIVATE HF TTY CIRCUIT.

(T1)-5, (T2) 5-20, (T3) 20-30, (T4)-30  
-----

FXP:

CCC-4-SF SYSTEM CONTROL SHIP TERMS TTY

CCC-8-SF TELETYPE CKT PROCEDURES

CCC-34-SF SYSTEM CONTROL - BLACK AUDIO SYSTEM (BAS)

-----  
- ATTAINABLE GOAL STANDARD REQUIRED IS T2.  
-----

2.) CCS WILL GENERATE COMSPOT DETAILING HF TTY UPON FINEX.  
OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF EFFECTIVENESS  
RESULTS VIA **Strike Group** CAS II: **indicate IP address.**//  
**Downgrading instructions in accordance with SECNAV M5510.36 (June  
2006)**

**DRILL PACKAGE INDIA - OTAT/OTAR ACTIVATION**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG INDIA) OTAT/OTAR ACTIVATION AND THE CRITERIA FOR MEASURING EFFECTIVENESS OF THE BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.
- A. EXERCISE: OTAT/OTAR RELAY
- B. OSE: **Strike Group Commander**
- C. OTC: **Strike Group Commander**
- D. OCE: **USS CV/CVN, LHA/LHD (SEC) USS CG**
- G. PARTICIPANTS: **Strike group units**
- NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN.
- I. TIME ZONE: ALL TIMES ARE ZULU
- J. COMEX: IAW SOE
- JJ. FINEX: IAW SOE
- N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED
- U. COMMUNICATIONS: VOICE COMMS/SIPR CHAT
- A. COORDINATION CIRCUITS:
1. PRI COORD:
2. SEC COORD:
3. EHF PTP
- V. INSTRUCTIONS:
- V.1. ALL UNITS MUST BE PREPARED TO ACTIVATE DESIGNATED CIRCUIT LINE NUMBER UPON REQUEST VIA COMSPOT AS DIRECTED BY THE COMMUNICATION CONTROL SHIP. HF PREDICTION AND PROPAGATION WILL BE DETERMINED PRIOR TO EXECUTION OF DRILL WHEN CONDUCTING DRILLS ON A HF CIRCUIT. CCS WILL GENERATE HF PREDICTION MESSAGE TO SUPPORT THIS EXERCISE.
- V2. CCS WILL CONDUCT ROLL CALL 15 MIN PRIOR TO COMEX. EACH UNIT WILL CALL UP AND ADVISE READABILITY ADVISING READABILITY. ONCE AMPLE CALL UPS ARE RECEIVED, CCS WILL TRANSMIT OTAT UTILIZING NAG-16. CCS WILL TRANSMIT THE OTAT THREE CONSECUTIVE TIMES. UPON THE LAST TRANSMITTAL, CCS WILL CALL UP ALL UNITS IF IN RECEIPT OF OTAT TRANSMISSION. A SECOND TRANSMITTAL OF OTAT CAN BE CONDUCTED AT THE DISCRETION OF CCS IF WITHIN THE NMTL TIME LIMIT. ALL UNITS WILL PROVIDE TIME OF RECEIPT VIA IMMEDIATE COMSPOT.
- ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST **CV/CVN, LHA/LHD** STRIKE GROUP'S ABILITY TO CONDUCT OTAT/OTAR TO MEET NMETL/NTA STANDARDS ISO COMPTUEX OBJECTIVES.

-----  
 - GOAL TO SUCCESSFULLY TRANSMIT OTAT/OTAR.  
 -----

C4I PKG INDIA (CCS OTAT/ALT CCS OTAT) (INITIATE OTAT SCENARIO)

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

NMETL/NTA(S)

S1. COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARDS:

FXP EXERCISE(S)

- OTAT TO SG VIA KYV-5 AND KY-58
- COMMUNICATION CONTROL SHIP WILL INITIATE OTAT ROLL CALL.
- UPON RECEIPT BY ALL UNITS, CCS WILL DIRECT USAGE OF OTAT RECEIVED AND ADVISE WHEN TO ACTIVATE DESIGNATED CIRCUIT.
- LOAD EFFECTIVE CRYPTO AND CONDUCT READABILITY CHECK VIA THE DESIGNATED CIRCUIT.

-----  
(S1H.) TIME IN (MINUTES) TO DEMONSTRATE OTAT.

- (T1) = 5, (T2) = 6-10, (T3) = 11-15, (T4) = 15.
- NECOS WILL ORDER THE ACTIVATION OF DESIGNATED NET FOR ALL UNITS.
- WHEN DIRECTED BY NECOS ALL UNITS WILL INITIATE OTAT.
- NECOS WILL DIRECT ALL UNITS TO EXIT OTAT.

-----  
---

FXP:  
CCC-30-SF OVER THE AIR TRANSFER AND OVER THE AIR REKEY  
CCC-6-SF RADIO TELEPHONE DRILLS  
CCC-5-SF SYSTEM CONTROL - SECURE/NONSECURE VOICE SYSTEMS

-----  
- ATTAINABLE GOAL STANDARD REQUIRED IS T2.  
-----

2. CCS WILL PROVIDE GRADE STANDARDS AND MEASURES OF EFFECTIVENESS RESULTS VIA **Strike Group** CAS II: **indicate IP address.// Downgrading instructions in accordance with SECNAV M5510.36 (June 2006).**

**DRILL PACKAGE JULIETT - RESTORE UHF DAMA**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG JULIETT) FOR UHF DAMA. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

- A. PROVIDE RESTORE UHF DAMA.
- B. OSE: **Strike Group Commander**
- C. OTC: **Strike Group Commander**
- D. OCE: **USS CV/CVN, LHA/LHD (SEC) USS CG**
- G. PARTICIPANTS: **Strike group units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN IAW REF B (MTO).

- I. TIME ZONE: ALL TIMES ARE ZULU
- J. COMEX: IAW SOE (NO NOTICE)
- JJ. FINEX: IAW SOE
- N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

-----  
 U. COMMUNICATIONS: PRIMARY WARFARE COMMANDERS VOICE AND CHAT CIRCUITS AS DESIGNATED IN **CV/CVN, LHA/LHD** STRIKE GROUP EFFECTIVE OPTASK COMMS ISO **exercise/evolution**.

- A. COORDINATION CIRCUITS:
  - 1. PRI COORD:
  - 2. SEC COORD:

V. INSTRUCTIONS:

-----  
 ZZ. 1. THIS EXERCISE IS DESIGNED TO TEST STRIKE GROUP ABILITY TO COME UP ON UHF DAMA TO MEET NMETL/NTA STANDARDS ISO **exercise/evolution** OBJECTIVES.

-----  
 - MAINTAIN ATTAINABLE GOAL STANDARD REQUIRED OF T2.

-----  
 - DETERMINE SINGLE DAMA CIRCUIT TO BE AFFECTED.

-----  
 - UNEXPECTED LOSS OF DAMA CIRCUITS MAY OCCUR.

-----  
 - CWC CMD/CUDIXS/CSG CMD NET/SATHICOM ARE SOME OF THE CIRCUITS TO BE DISTRIBUTED AT ANY GIVEN TIME WITH OUT NOTICE. UNITS WILL BE PROMPTED AND RESTORED INITIATED BY GUIDANCE OF CCS.

-----  
 - PROVIDED BELOW ARE THE LISTED NMETL/NTA OBJECTIVES WHICH WILL BE OBSERVED.

-----  
 NMETL/NTA(S)

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

S1. COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARDS:



S1B. TIME (MINUTES) TO RESTORE FROM LOSS OF VITAL DAMA  
PRIORITIZED CIRCUITS IAW SHIPBOARD SOP. (T1) - 10, (T2) - 10-20,  
(T3) - 20-30, (T4) - 30

---

FXP:

CCC-4-SF SYSTEM CONTROL SHIP TERMS TTY  
CCC-5-SF SYSTEM CONTROL SECURE VOICE  
CCC-6-SF RADIO-TELEPHONE DRILLS  
CCC-8-SF TELETYPE CKT PROCEDURES  
CCC-24-SF SYSTEMS CONTROL NARROWBAND/WIDEBAND SATELLITE  
COMMUNICATIONS SYSTEMS  
CCC-34-SF SYSTEM CONTROL - SINGLE AUDIO SYSTEM (SAS) AND BLACK  
AUDIO SYSTEM (BAS)  
CCC-39-SF SYSTEM CONTROL - 5KHZ/DAMA SATELLITE COMMUNICATIONS  
SYSTEMS

---

2. CCS WILL GENERATE COMSPOT DETAILING DAMA VOICE/DATA  
CONNECTIVITY UPON FINEX. OCE WILL PROVIDE GRADE STANDARDS AND  
MEASURES OF EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group**  
CAS II: **indicate IP address.**//  
**Downgrading instructions in accordance with SECNAV M5510.36 (June**  
**2006.**

**DRILL PACKAGE KILO - ACTIVATE AND  
INITIATE DEMAND CALL VIA KY-68**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG KILO) FOR KY-68 OF EFFECTIVENESS GRADING CRITERIA. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

- A. PROVIDE KY-68.
- B. OSE: **Strike Group Commander**
- C. OTC: **Strike Group Commander**
- D. OCE: **USS CV/CVN, LHA/LHD (SEC) USS CG**
- G. PARTICIPANTS: **Strike group units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN REF B (MTO).

- I. TIME ZONE: ALL TIMES ARE ZULU
- J. COMEX: IAW SOE (NO NOTICE)
- JJ. FINEX: IAW SOE
- N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

-----  
U. COMMUNICATIONS: PRIMARY WARFARE COMMANDERS VOICE AND CHAT CIRCUITS AS DESIGNATED IN **CV/CVN, LHA/LHD** STRIKE GROUP EFFECTIVE OPTASK COMMS ISO **exercise/evolution**.

- A. COORDINATION CIRCUITS:
  - 1. PRI COORD:
  - 2. SEC COORD:

V. INSTRUCTIONS:

-----  
ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST STRIKE GROUP ABILITY TO ACTIVATE AND INITIATE KY-68 ON DEMAND CALLS TO MEET NMETL/NTA STANDARDS ISO **exercise/evolution** OBJECTIVES.

-----  
- MAINTAIN ATTAINABLE GOAL STANDARD REQUIRED OF T2.

-----  
- ACTIVATE AND INITIATE ON DEMAND CALL VIA KY-68  
END USER CONTACT INFO:

CUSNC TFCC WATCH  
DSN 318-439-4006  
DRSN 721-0099  
CENTCOM TCCC CWO  
DSN 318-439-3875  
DRSN 539-2504  
C6F TFCC WATCH  
DRSN 626-2356  
NCTS NAPLES COW  
DSN 314-626-3725/3350

This information will be unique to each AOR.
--

-----  
- PROVIDED BELOW ARE THE LISTED NMETL/NTA OBJECTIVES WHICH WILL

BE OBSERVED.

-----  
C4I PKG KILO (KY-68) (ACTIVATE AND INITIATE ON DEMAND  
CALL)  
NMETL/NTA(S)

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

S1. COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARDS:

TIME IN (MINUTES) TO ESTABLISH DRSN CONNECTIVITY WITH END USER.  
T1=<15, T2=15-25, T3=25-40, T4=>40.

ARE UNITS ABLE TO ESTABLISH VOICE COMMUNICATION WITH C5F/C6F AOR  
END USER VIA LONG LOCAL TERMINATION?  
T1=YES, T2=N/A, T3=N/A, T4=NO.

-----  
DEMONSTRATE ABILITY TO PERFORM ACTIVATION OF KY-68 CALL. T1=YES,  
T2=N/A, T3=N/A, T4=NO.  
-----

-  
- NECOS WILL ORDER THE ACTIVATION OF DESIGNATED CKT FOR ALL  
UNITS.  
-----

CCC-25-SF SUPER HIGH FREQUENCY SATELLITE COMMUNICATIONS  
-----

2.) OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF  
EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS II:

**indicate IP address.//**

**Downgrading instructions in accordance with SECNAV M5510.36 (June  
2006.)**

**DRILL PACKAGE LIMA - CSG/ESG BANDWIDTH MANAGEMENT**

1. PROVIDED IS THE STANDING PRE-EX FOR C4I PKG LIMA BANDWIDTH MANAGEMENT. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

- A. PROVIDE BANDWIDTH MANAGEMENT.
- B. OSE: **Strike Group Commander**
- C. OTC: **Strike Group Commander**
- D. OCE: **USS CV/CVN, LHA/LHD (SEC) USS CG**
- G. PARTICIPANTS: **Strike group units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN REF B (MTO).

- I. TIME ZONE: ALL TIMES ARE ZULU
- J. COMEX: IAW SOE (NO NOTICE)
- JJ. FINEX: IAW SOE
- N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

-----  
 U. COMMUNICATIONS: PRIMARY WARFARE COMMANDERS VOICE AND CHAT CIRCUITS AS DESIGNATED IN STRIKE GROUP EFFECTIVE OPTASK COMMS ISO **exercise/evolution**.

- A. COORDINATION CIRCUITS:
  - 1. PRI COORD:
  - 2. SEC COORD:

V. INSTRUCTIONS:

-----  
 ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST STRIKE GROUP ABILITY TO ADJUST THE BANDWIDTH MANAGEMENT TO MEET NMETL/NTA STANDARDS ISO **exercise/evolution** OBJECTIVES.

- MAINTAIN ATTAINABLE GOAL STANDARD REQUIRED OF T2.
- ADJUST AND MANAGE STAFF B/W PLAN.
- PROVIDED BELOW ARE THE LISTED NMETL/NTA OBJECTIVES WHICH WILL BE OBSERVED.

-----  
 --  
 C4I PKG LIMA (BANDWIDTH MANAGEMENT)  
 (ADJUST AND MANAGE STAFF B/W PLAN)

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS  
 NMETL/NTA(S)

-----  
 DEMONSTRATE ABILITY TO PERFORM ADJUSTMENT AND MANAGE STAFF B/W PLAN.

T1=YES, T2=N/A, T3=N/A, T4=NO.  
 -----

(NECC)

TIME IN (MINUTES) TO LOAD THE CORRECT NECC COMM CONFIGURATION FOR CURRENT AOR. T1=<15, T2=15-30, T3=30-45, T4=>45.

- NECOS WILL PROVIDE STATUS ON ALL UNITS REACHABLE VIA NECC.
- NECOS WILL CONDUCT OTO WITH ALL REACHABLE UNITS.
- NECOS WILL HANDOVER NECOS VIA NECC.

-----  
TERMINAL FAULT STATUS

TIME IN (MINUTES) TO PERFORM AUTOMATIC TEST SEQUENCE (ATS) TO ENSURE NO FAULTS ARE PRESENT. T1=<5, T2=6-7, T3=8-9, T4=>9.

- ENSURE A QUALIFIED VTC TECH IS PRESENT WITH THE VTC OPERATOR WHEN CONDUCTING ANY TESTING.
- NECOS WILL DESIGNATE WHEN EACH UNIT WILL CONDUCT ATS.
- UPON COMPLETION PROVIDE STATUS OF ATS FAULTS VIA COMSPOT.

-----  
TIME IN (MINUTES) TO PERFORM ADJUSTMENT AND MANAGE STAFF B/W PLAN. T1 <45, T2 45 - 75, T3 75 - 180, T4 >180.

- NECOS WILL ORDER THE ACTIVATION OF DESIGNATED NET FOR ALL UNITS.

-----  
2.) OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS II: **indicate IP address.**//

**Downgrading instructions in accordance with SECNAV M5510.36 (June 2006)**

**DRILL PACKAGE MIKE - CENTRIXS REPLICATION /  
CROSS DOMAIN SOLUTION**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG MIKE) FOR CROSS-DOMAIN MAIL GUARD. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. EXERCISE: SIPR TO CENTRIXS CROSS DOMAIN SOLUTION

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: **USS CV/CVN, LHA/LHD (SEC) USS CG**

G. PARTICIPANTS: **TBD**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN IAW REF A THRU J SCHEDULE OF EVENTS (SOE).

I. TIME ZONE: ALL TIMES ARE ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

-----  
U. COMMUNICATIONS: PRIMARY WARFARE COMMANDERS VOICE AND CHAT CIRCUITS AS DESIGNATED IN **CV/CVN, LHA/LHD** STRIKE GROUP EFFECTIVE OPTASK COMMS ISO **exercise/evolution..**

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD: CENTRIXS SAMETIME CHAT (IP: )

V. INSTRUCTIONS:

-----  
ZZ.1) THIS EXERCISE IS DESIGNED TO TEST STRIKE GROUP ABILITY TO DEMONSTRATE CENTRIXS REPLICATION TO MEET NMETL/NTA STANDARDS ISO **exercise/evolution** OBJECTIVES.

-----  
- PROVIDED BELOW ARE THE LISTED NMETL/NTA OBJECTIVES WHICH WILL BE OBSERVED.

-----  
- NMETL/NTA(S)

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

-----  
-. COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARD:

TIME IN (MINUTES) TO ESTABLISH CENTRIXS CONNECTIVITY WITH STRIKE GROUP UNITS VIA A CHOSEN ENCLAVE AND SENDING AN EMAIL TO ALL UNITS WITHIN THE SG TO CONFIRM RECEIPT AND OPERATION OF THE SELECTED ENCLAVE.

-----  
(T1) < 20, (T2) 20-30, (T3) 30-45, (T4) > 45.  
-----

ARE ALL EMAIL ADDRESSES FOR THE STRIKE GROUP UPDATED WITHIN THE MAIL GUARD SYSTEM FOR EACH ENCLAVE?

-----  
(T1) = YES, (T2) = N/A, (T3) = N/A, (T4) = NO.  
-----

FXP:

CCC-25-SF SUPER HIGH FREQUENCY SATELLITE COMMUNICATIONS  
-----

2). CCS WILL GENERATE COMSPOT DETAILING CROSS-DOMAIN CONNECTIVITY UPON FINEX. OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS II:

**indicate IP address.//**

**Downgrading instructions in accordance with SECNAV M5510.36 (June 2006).**

**DRILL PACKAGE NOVEMBER - COMMUNICATE VIA CENTRIXS EMAIL**

1. PROVIDED IS THE STANDING PRE-EX FOR CENTRIXS (**enclave**) CHECKS. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRAPAC AND COMSTRKFORTRALANT CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. PERFORM AND OBSERVE IN HOUSE SYSTEM CHECKS ON CENTRIXS (**enclave**)

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: (PRI) USS **CV/CVN, LHA/LHD** (SEC) **AFLOAT COALITION UNIT**

G. PARTICIPANTS:

I. TIME ZONE: ALL TIMES ARE ZULU

J. COMEX:

JJ. FINEX:

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

-----  
 --  
 U. COMMUNICATIONS: PRIMARY WARFARE COMMANDERS CHAT CIRCUITS AS DESIGNATED IN STRIKE GROUP EFFECTIVE OPTASK COMMS ISO **exercise/evolution.**

A. COORDINATION CIRCUITS:

1. PRI COORD:

V.1 INSTRUCTIONS:

-----  
 --  
 ZZ. 1. THIS EXERCISE IS DESIGNED TO TEST STRIKE GROUP ABILITY TO USE A SELECTED ENCLAVE OF CENTRIXS TO ESTABLISH CENTRIXS CONNECTIVITY WITH STRIKE GROUP UNITS VIA A CHOSEN ENCLAVE WITHIN NMETL/NTA STANDARDS AND OPERATIONAL OBJECTIVES.  
 -ALL SHIPS ACTIVATE CENTRIXS **enclave**. CONCENTRATE ON IN HOUSE SYSTEM CHECKS ON THE \_\_\_\_\_ ENCLAVES.  
 -PROVIDE THE STAFF WITH ALL EMAIL ACCOUNTS FOR TESTING PURPOSES.  
 -EMAIL ADDRESSES SHOULD BE EMAILED TO **Strike Group SIPR address.**  
 -VERIFY CORRECT CRYPTO IS ON HAND.  
 -INSTALL ALL ACTIVE X AND JAVA PATCHES.  
 -CENTRIXS **enclave** HOMEPAGE IS \_\_\_\_\_  
 -ENSURE APPROPRIATE CAS ACCOUNTS (CO, XO, TAO, BWC, RADIO, ETC.) ARE CREATED.  
 -ENTER SAMETIME CHAT MEETING ROOM (**enter name of chat room**)  
 ALL ACTIONS SET FORTH IN THIS MESSAGE MUST BE COMPLETED IN ORDER TO SUCCESSFULLY COMPLETE FUTURE COMMUNICATIONS WITH CENTRIXS. REPORT COMPLIANCE WITH THIS PRE-EX TO THE STRIKE GROUP VIA IMMEDIATE COMSPOT.

-----  
 - PROVIDED BELOW ARE LISTED NMETL/NTA OBJECTIVES WHICH WILL BE OBSERVED.  
 -----

XM (S8D). TIME (HOURS) TO SHIFT TO THE " \_\_\_\_\_ " ENCLAVE USING SG SOP, AND VERIFY ESTABLISHED CONNECTIVITY WITH ALL STRIKE GROUP



UNITS BY EXCHANGING EMAILS.

T1<2, T2<3, T3<4, T4>4.

-----  
XM (S8I). WHILE IN THE \_\_\_\_\_ " ENCLAVE CONFIRM/VERIFY  
THE FOLLOWING FOR ALL STRIKE GROUP UNITS:

T1 >93%, T2 >86%, T3 =>79%, T4 < 79%

-APPROPRIATE PERSONNEL AND WATCHSTATIONS HAVE A REGISTERED  
EMAIL ADDRESS.

-ABILITY TO ACCESS THE CAS HUB SITE AND THE STRIKE GROUP CAS  
SITE

-PROPERLY CONNECT/USE SAMETIME CHAT

-LATEST VERSION OF SAMETIME CHAT LOADED ON ALL WORKSTATIONS  
INCLUDING THE PDC AND BDC

-LATEST VERSION OF NORTON ANTIVIRUS LOADED ON ALL WORKSTATIONS  
INCLUDING THE PDC AND BDC

-SYSTEM CLOCK SET TO ZULU TIME

-STRIKE GROUP/SHIP SOP (WITH CHECKLIST) ADDRESSING THE STEP-BY-  
STEP PROCESS TO SHIFT ENCLAVES

-CENTRIXS PROPERLY AND ADEQUATELY ADDRESSED IN THEIR OPTASK  
IM/COMMS/CHAT

-PROPER LABELING, STORAGE AND ACCOUNTABILITY OF ALL AVAILABLE  
HARD DRIVES, INCLUDING THE PDC, BDC AND LAPTOP DRIVES.

-----  
FXP:

CCC-25-SF SUPER HIGH FREQUENCY SATELLITE COMMUNICATIONS  
-----

//

**DRILL PACKAGE OSCAR - RIVER CITY**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG OSCAR) RIVER CITY. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA

NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. RIVER CITY WARFARE COMMANDER FREQUENCY SHIFTS AND KICKS.

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: (PRI) USS **CV/CVN, LHA/LHD** (SEC) **USS CG**

G. PARTICIPANTS: **Strike Group Units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN IAW REF A AND B SCHEDULE OF EVENTS (SOE).

I. TIME ZONE: ALL TIMES ARE ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

U. COMMUNICATIONS: PRIMARY WARFARE COMMANDERS VOICE AND CHAT CIRCUITS AS DESIGNATED IN **CV/CVN, LHA/LHD** STRIKE GROUP EFFECTIVE OPTASK COMMS ISO **exercise/evolution**.

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD:

V. INSTRUCTIONS:

V.1 EACH IAM WILL TAKE NECESSARY PRECAUTION AND ENSURE RIVER CITY IS FULLYWARFARE COMMANDER WILL BE RESPONSIBLE FOR INITIATING FREQUENCY SHIFTS OR KICKS AT LEAST TWICE DAILY UTILIZING ASSIGNED CIRCUITS AND FREQUENCIES PROVIDED VIA THE EFFECTIVE OPTASK COMMS.  
- ALL IT(S) IN MAINCOMM WILL BE READY TO ASSIST INDIVIDUAL WARFARE CMDRS WITH DETERMINING BEST COURSE OF ACTION AND EXECUTION WHEN SHIFTING FREQUENCIES BASED ON EQUIPMENT STATUS AND AVAILABILITY OF RESOURCES.

-----  
ZZ. 1.) THIS EXERCISE IS DESIGNED TO TEST **CV/CVN, LHA/LHD** STRIKE GROUP'S ABILITY TO SHIFT FREQUENCIES AND MEET NMETL/NTA STANDARDS ISO **exercise/evolution** OBJECTIVES.  
-----

- GOAL WILL BE TO SHIFT FREQUENCIES/CIRCUITS AS DIRECTED BY WARFARE CMDRS.  
-----

- MAINTAIN ATTAINABLE GOAL STANDARD REQUIRED OF T2.  
-----

- GOAL WILL BE TO MAINTAIN ASSIGNED AND GUARDED WARFARE CMDR NETS. ALL CIRCUITS MUST BE ACTIVATED AS DIRECTED ISO EXECUTING C4I EXERCISE EVENT.  
-----

- PROVIDED BELOW ARE LISTED THE NMETL/NTA OBJECTIVES WHICH WILL BE OBSERVED.

-----  
C4I PKG OSCAR (RIVERCITY IMPLEMENTATION)  
(SET VARIOUS RIVERCITY CONDITIONS)

NMETL/NTA(S)

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS

S1.- COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARDS  
-----

NTA 5.5.5 PERFORM INFORMATION ASSURANCE

S1. COMMUNICATIONS CONTROL SHIP (CCS) EFFECTIVENESS STANDARDS:  
-----

S4. SET/REPORT RIVERCITY CONDITION TO IWC.

S4A. TIME TO SET (MINUTES) RIVERCITY CONDITION 3.  
(T1)-9, (T2) 9-10, (T3) 10-12, (T4) 12

S4B. TIME TO SET (MINUTES) RIVERCITY CONDITION 2.  
(T1)-7, (T2) 7-8, (T3) 8-10, (T3) 10

S4C. TIME TO SET (MINUTES) RIVERCITY CONDITION 1.  
(T1)-4, (T2) 4-5, (T3) 5-7, (T4)-7  
-----

2). CCS WILL GENERATE COMSPOT DETAILING RIVERCITY IMPLEMENTATION  
UPON FINEX. OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF  
EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS II:

**indicate IP address.//**

**Downgrading instructions in accordance with SECNAV M5510.36 (June  
2006.**

## DRILL PACKAGE PAPA - INFOCON

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG PAPA) INFOCON EXERCISE.

THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE.

A. (C) EXERCISE TO BE CONDUCTED: INFOCON DRILL

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: (PRI) USS **CV/CVN, LHA/LHD** (SEC) **USS CG**

G. PARTICIPANTS: **Strike Group Units**

NOTE: ALL PARTICIPANTS MAY NOT BE ASSIGNED TO PARTICIPATE IN EACH C4I STANDING PRE-EX EVENT AS INDICATED IN THE PARTICIPANTS COLUMN IAW (MTO).

I. (U) TIME ZONE: ALL TIMES ARE ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ. FINEX: IAW SOE

N. AREA OF EXERCISE:

U. COMMUNICATIONS: PRIMARY WARFARE COMMANDERS VOICE AND CHAT CIRCUITS AS DESIGNATED IN **CV/CVN, LHA/LHD** STRIKE GROUP EFFECTIVE OPTASK COMMS ISO **exercise/evolution**.

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD:

3. TER COORD:

COORDINATION CIRCUITS ARE SECURED DUE TO RIVER CITY IMPLEMENTATION, REPORTS WILL BE MADE VIA VOICE CIRCUIT.

V. INSTRUCTIONS:

V.1. (C) BACKGROUND: INFOCON IS A COMPREHENSIVE COMPUTER NETWORK MANAGEMENT POSTURE BASED ON THE STATUS OF INFORMATION SYSTEMS, MILITARY OPERATIONS, AND ADVERSARY CAPABILITIES, INTENT AND ACTIONS. EACH INFOCON LEVEL INCLUDES MEASURES TO UNIFORMLY HEIGHTEN OR REDUCE CND POSTURE, TO DEFEND AGAINST COMPUTER NETWORK ATTACKS AND TO MITIGATE DAMAGE TO THE DOD INFORMATION INFRASTRUCTURE, SPECIFICALLY

COMPUTER NETWORKS. THE PURPOSE OF THIS EXERCISE IS TO ENSURE THAT **strike group** UNITS HAVE VALID USER GROUPS, THAT ESSENTIAL CONNECTIVITY WITH THE OFF-SHIP CHAIN OF COMMAND IS MAINTAINED, AND THAT NETWORK MANAGERS AND IAMS ARE PROFICIENT AT SETTING AND CHANGING INFOCON LEVELS AND USE OF THE IA TOOL KIT.

V.2. (C) PROCEDURES: ALL UNITS SHALL SUBMIT INTRUSION DETECTION SYSTEM BASELINES NLT COMEX OF EVENT AND BE LOGGED IN TO THE **strike group commander IW** CHATROOM

V.3. UPON COMEX, IWC WILL DIRECT CHANGES TO INFOCON LEVELS AND UNITS WILL PASS ATTAINMENT REPORTS VIA CHAT. IF CHAT IS LOST, ALL UNITS ASSUME INFOCON B AT COMEX, ESTABLISH INFOCON CHARLIE AT 30 MIN AFTER COMEX. FOR AT LEAST 30 MINUTES, THEN SWITCH BACK TO INFOCON B UNTIL FINEX. DURING ALL PHASES OF THIS EXERCISE, SHIPS ARE TO TEST CONNECTIVITY OF CRITICAL NODES IN THE COMMAND, I.E. CO/XO/OPSO/TAO/SUPPO/CMC AND MONITOR SNORT BASELINES FOR NETWORK

SCANS AND INTRUSIONS BY NIOC CND TRAINERS.

A. ALL UNITS WILL MAKE ATTAINMENT REPORTS TO IWC VIA CHAT ON THE SECONDFLT SERVER. THE IP ADDRESS IS 206.36.162.13 AND THE CHATROOM IS **strike group\_IWC\_COORD**.

B. FOLLOW GUIDANCE AS PROMULGATED IN **Strike Group Commander** OPORD 6000-04 AND NIOC CND TACMEMO 3-13.1-03 AS WELL AS LOCAL INFOCON SOP'S WHEN SETTING EACH INFOCON LEVEL. COMMANDS REQUIRING ELECTRONIC REFERENCES REFER TO STRIKE GROUP'S CAS SITE.

C. PRE-DEFINED USER GROUP METHODOLOGY WILL BE USED TO ENSURE OPERATIONALLY ESSENTIAL PERSONNEL MAINTAIN ACCESS THROUGHOUT INFOCON SETTINGS.

D. EACH UNIT WILL ASSESS IMPACT TO OPERATIONAL CAPABILITY DURING DIRECTED INFOCON LEVEL AND PROVIDE POSTEX LESSONS LEARNED TO ORIG VIA EMAIL WITHIN 48 HRS OF FINEX.

4. IN THE EVENT OF REAL-WORLD CONTINGENCIES, ANY UNIT MAY ENACT RELAXATION OF RESTRICTIVE INFOCON LEVELS TO PROPERLY POSTURE SYSTEMS IN RESPONSE TO ON-GOING OPERATIONS.

5. CCS WILL GENERATE COMSPOT DETAILING RIVERCITY IMPLEMENTATION UPON FINEX. OCE WILL PROVIDE GRADE STANDARDS AND MEASURES OF EFFECTIVENESS RESULTS TO BE POSTED VIA **Strike Group** CAS II:

**indicate IP address.//**

**Downgrading instructions in accordance with SECNAV M5510.36 (June 2006).**

**DRILL PACKAGE QUEBEC - CND INCIDENT ASSURANCE MONITORING**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG QUEBEC) CND INCIDENT REPORTING ACTIVATION AND THE CRITERIA FOR MEASURING EFFECTIVENESS OF THE BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE *Strike Group* CAS SITE.

- A. EXERCISE: CND INCIDENT AND REPORTING SCENARIO
- B. OSE: *Strike Group Commander*
- C. OTC: *Strike Group Commander*
- D. OCE: (PRI) USS *CV/CVN, LHA/LHD* (SEC) *USS CG*
- G. PARTICIPANTS: *Strike Group Units*
- I. TIME ZONE: ALL TIMES ARE ZULU
- J. COMEX: IAW SOE (NO NOTICE)
- JJ. FINEX: IAW SOE
- N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED
- U. COMMUNICATIONS: SIPR CHAT/VOICE COMMS
  - A. COORDINATION CIRCUITS:
    - 1. PRI COORD:
    - 2. SEC COORD:

V. INSTRUCTIONS:

V.1 BACKGROUND: COMPUTER VIRUSES, TROJAN HORSES, AND MALICIOUS CODE INCIDENTS, KNOWN OR SUSPECTED NETWORK INTRUSIONS AND OTHER SUSPICIOUS COMPUTER INCIDENTS MUST BE REPORTED TO NCDOP OPNAVINST 2201.2. THIS EXERCISE IS DESIGNED TO FLEX THE COMPUTER INCIDENT REPORTING SYSTEM.

V.2. SCENARIO: YOUR COMMAND RECEIVED THE ZOTOB.E TROJAN FROM A STAFF'S RECENT EMBARKATION WHILE ATTEMPTING TO EMBARK AND CONNECT TO AN NMCI HOST. OVER TWO DOZEN WORKSTATIONS HAVE BEEN INFECTED AND HAD TO BE MANUALLY CLEANED.

V3. SIX HUNDRED TWENTY FIVE MAN-HOURS WERE EXPENDED WHILE ISOLATING THE CAUSE OF THE OUTAGE AND CLEANING INFECTED WORKSTATIONS. FOR THE PUPOSE OF THIS EXERCISE, DRAFT AN INCIDENT REPORT IAW GUIDANCE FROM OPNAVINST 2201.2. INCLUDE YOUR EXCHANGE SERVER ANTI-VIRUS SOFTWARE VERSION, LATEST SIGNATURE DATE AND POC INFO. EXERCISE WILL BE EVALUATED ON TIMELINESS OF SUBMISSION AND ACCURACY OF REPORT.

-----  
 ZZ.1. THIS EXERCISE IS DESIGNED TO TEST STRIKE GROUP ABILITY TO PERFORM BELOW NTA'S.  
 -----

C4I PKG QUEBEC (CND INCIDENT AND REPORTING SCENARIO)  
 (INJECT, IMPLEMENT, AND DETECT CND TASKER)

NMETL/NTA(S)  
 -----

NTA 5.5.5 PERFORM INFORMATION ASSURANCE

A. ARE SUFFICIENT INCIDENT REPORTING PROCEDURES ESTABLISHED, IMPLEMENTED, AND TESTED NMETL STANDARDS OBSERVED ARE:  
 -----

--

NTA 5.5.5 PERFORM INFORMATION ASSURANCE

-----  
CND OBJECTIVES ARE INTEGRATED INTO TRAINING AND DRILLS.  
(T1) -YES, (T2) -N/A, (T3) -N/A, (T4) -NO.  
-----

COMPUTER INCIDENT REPORTING PROCEDURES INTEGRATED AND  
EVALUATED WITHIN THE COMMAND EXERCISES AND OPERATIONS.  
(T1) -YES, (T2) -N/A, (T3) -N/A, (T4) -NO.  
-----

2.. RESULTS OF EXERCISE WILL BE PROVIDED SEPCOR VIA IMMEDIATE  
COMSPOT.//

***Downgrading instructions in accordance with SECNAV M5510.36 (June  
2006.***

**DRILL PACKAGE ROMEO - INFORMATION ASSURANCE MONITORING**

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG ROMEO) FOR IA MONITORING. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

- A. EXERCISE: IA MONITORING SCENARIO
- B. OSE: **Strike Group Commander**
- C. OTC: **Strike Group Commander**
- D. OCE: (PRI) USS **CV/CVN, LHA/LHD** (SEC) **USS CG**
- G. PARTICIPANTS: **Strike Group Units**
- I. TIME ZONE: ALL TIMES ARE ZULU
- J. COMEX: IAW SOE (NO NOTICE)
- JJ.FINEX: IAW SOE
- N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED
- U. COMMUNICATIONS: CHAT, MESSAGE.
  - A. COORDINATION CIRCUITS:
    - 1. PRI COORD:
    - 2. SEC COORD:

V. INSTRUCTIONS:

V1. (C) BACKGROUND: INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE ARE COMPREHENSIVE EVALUATED EXERCISES TO DEFEND AGAINST COMPUTER NETWORK ATTACKS/INTRUSIONS AND TO MITIGATE DAMAGE TO THE DOD INFORMATION INFRASTRUCTURE, SPECIFICALLY COMPUTER NETWORKS. THE PURPOSE OF THIS EXERCISE IS TO ASSESS THE CURRENT VULNERABILITIES OF **Strike Group** COMMANDS, TO ASSESS SHIPBOARD PERSONNEL ACTIONS TO PROTECT SHIPBOARD NETWORKS, THAT OFF-SHIP CONNECTIVITY WITH OTHER STRKGRU UNITS IS MAINTAINED, AND THAT NETWORK AND SECURITY MANAGERS ARE PROFICIENT AT USING THE INFORMATION ASSURANCE (IA) TOOL KIT.

V2. (C) PROCEDURES:

ENSURE ALL APPROVED IAVA SOFTWARE PATCHES ARE INSTALLED, AND THAT INTRUSION DETECTION SYSTEM (IDS; SNORT OR REALSECURE) IS ACTIVE WITH LOGGING BEING MONITORED. ALL UNITS SHALL BE LOGGED IN TO THE **Strike Group** COMM COORD CHATROOM TWO HOURS PRIOR TO THE CNDEX EACH DAY. REPORT SUSPICIOUS ACTIVITY VIA CND INCIDENT REPORTS AND TO IWC VIA CHAT. DURING ALL PHASES OF THIS EXERCISE, SHIPS ARE TO MONITOR IDS FOR NETWORK SCANS AND INTRUSIONS.

V3. (U) REPORTING REQUIREMENTS:

REPORT POSSIBLE INTRUSIONS USING FORMAT SPECIFIED IN REF F. WHILE INTRUSIONS ARE OCCURRING DURING AN EXERCISE PERIOD, PARTICIPANTS SHOULD CONSIDER ALL INTRUSIONS AS ACTUAL INTRUSIONS UNTIL OTHERWISE DETERMINED BY NCDIC.

-----

V.4. ALL UNITS SHALL VERIFY PASSWORD CRACK PROGRAM IS AVAILABLE. PROGRAM SHOULD RUN FOR APPROXIMATELY ONE HOUR. ENSURE ACCOUNTS WITH CRACKED PASSWORDS ARE DISABLED AND THAT NO DEFAULT PASSWORDS ARE ACTIVE. NLT **date/time**, PROVIDE A SUMMARY REPORT VIA RMG ON INFORMATION ASSURANCE TOOLKIT PASSWORD CRACKER. MESSAGE ACTION TO



**Commander Strike Group** (FOR DESRON SHIPS INFO COMDESRON **XX**) SHALL INCLUDE THE BELOW LISTED ITEMS.

A. PASSWORD CRACKING. STATE DATE AND TIME PASSWORD CRACK WAS RUN AND PROVIDE BELOW STATISTICS.

NUMBER OF UNCLASSIFIED PASSWORDS TOTAL

NUMBER OF UNCLASSIFIED PASSWORDS CRACKED TOTAL

NUMBER OF UNCLASSIFIED ADMINISTRATOR ACCOUNT PASSWORDS CRACKED

NUMBER OF CLASSIFIED PASSWORDS TOTAL

NUMBER OF CLASSIFIED PASSWORDS CRACKED TOTAL

NUMBER OF CLASSIFIED ADMINISTRATOR ACCOUNT PASSWORDS CRACKED

2. USERS WITH WEAK PASSWORDS SHOULD BE TRAINED ON PROPER PASSWORD CREATION AND ATTEND AN INFORMATION ASSURANCE REFRESHER COURSE.

3. COMMAND IA/CND REPORT. FOR ALL PARTICIPATING UNITS PROVIDE THE FOLLOWING INFORMATION VIA RMG:

A. LIST OF UNIT PERSONNEL PARTICIPATING IN THESE GROUP SAIL EXERCISE EVENTS BY NAME/RATE OR RANK/BILLET/PRD WHO HAVE RECEIVED CND TRAINING. LIST, BY EVENT NUMBER, THE **Strike Group** CND TRAINING EVENTS THE PERSON PARTICIPATED IN DURING

**exercise/evolution.**

TRAINING EVENT CODES:

1 - ATTENDED NIOC IA/CND AFLOAT, NIOC

2 - NAVY IAM COURSE GRADUATE

3 - CIVILIAN COMPUTER SECURITY CERTIFICATES OR EQUIVALENTS

4 - NETWORK SECURITY VULNERABILITY TECHNICIAN GRADUATE

5 - JOURNEYMAN NETWORKING CORE GRADUATE

6 - COMMAND WEBMASTER

EXAMPLE: M. MOORE/IT1/IAM/01MAR07/1,2,3,4,5,6/

B. DATE OF YOUR COMMAND'S LAST NCDQC ON-LINE SURVEY ON NIPR AND SIPR NETWORKS.

C. SUMMARY OF YOUR SIPR AND NIPR NETWORK PASSWORD POLICY. SUMMARY SHOULD INCLUDE THE FOLLOWING INFORMATION AT A MINIMUM.

1. CHANGE OF PASSWORD FREQUENCY.

2. MINIMUM PASSWORD HISTORY.

3. MINIMUM PASSWORD CHARACTERS.

4. # OF LOGON ATTEMPTS BEFORE LOCKOUT.

D. SIPR AND NIPR NETWORK ACCREDITATION STATUS. ARE YOUR NETWORKS FULLY ACCREDITED IAW THE DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY CERTIFICATION AND ACCREDITATION PROCESS (DITSCAP)? IF NOT, IS THERE AN INTERIM AUTHORITY TO OPERATE (IATO) IN EFFECT? WHAT IS THE DATE OF THE IATO?

E. CURRENT VERSION OF THE INFORMATION ASSURANCE TOOLKIT HELD ONBOARD.

F. COMMANDS INFORMATION ASSURANCE TRAINING PLAN. HOW ARE DON REQUIREMENTS MET?

G. DATE OF SYMANTEC ANTIVIRUS SIGNATURE ON YOUR NIPR AND SIPR SERVERS.

ZZ.1 THIS EXERCISE IS DESIGNED TO TEST STRIKE GROUP ABILITY TO CONDUCT IA MONITORING AND MEET NTA STANDARDS.

-----  
NTA STANDARDS TO BE OBSERVED:

NTA 5.5.5. INFORMATION ASSURANCE (IA) FOR INTERMEDIATE PHASE  
-----

IA OBJECTIVES ARE INTEGRATED INTO TRAINING AND DRILLS.

-----  
 T1=Yes, T2=N/A, T3=N/A, T4=NO  
 -----

DOES THE COMMAND HAVE THE TRAINING (I.E. NSVT, ANA ETC...) REQUIRED TO RECONSTRUCT UNAUTHORIZED ACTIVITY AND ATTACKS?

-----  
 T1=YES, T2=N/A, T3=N/A, T4=NO  
 -----

NTA 5.5.5. INFORMATION ASSURANCE (IA) for BASIC PHASE

-----  
 NUMBER OF FULL-TIME SYSTEM ADMINISTRATORS ASSIGNED TO MAINTAIN SYSTEMS WITH PROPER NEC'S.

-----  
 T1= YES, T2=N/A, T3=N/A, T4=NO  
 -----

PERCENT OF NETWORKS THAT COMPLETED CERTIFICATION AND ACCREDITATIONS (C&A) IAW DOD INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROCESS (DITSCAP). ADEQUATE ARCHITECTURE FOR SECURING SYSTEMS AND NETWORKS ARE IN PLACE.

-----  
 T1=100%, T2=N/A, T3=N/A, T4=<100%  
 -----

IA OBJECTIVES ARE INTEGRATED INTO COMMAND LEVEL TRAINING AND EXERCISES.

-----  
 1=YES, T2=N/A, T3=N/A, T4=NO  
 -----

DOES THE COMMAND HAVE A REGISTERED COPY OF THE FLEET IA TOOLKIT (Version 1.0).

-----  
 T1=YES, T2=N/A, T3=N/A, T4=NO  
 -----

NTA 5.5.5.1 COMPUTER NETWORK DEFENSE (CND) BASIC PHASE

-----  
 REGULAR AND PROACTIVE VULNERABILITY ANALYSIS, ASSESSMENTS AND EVALUATIONS PROGRAM TO IDENTIFY DEFICIENCIES. (NCDOC SCANNING).

-----  
 T1=YES, T2=N/A, T3=N/A, T4=NO  
 -----

DOES THE COMMAND ENFORCE STRONG PASSWORD MANAGEMENT AND CHANGE POLICY EVERY 90 DAYS.

-----  
 T1=Yes, T2=N/A, T3=N/A, T4=No.  
 -----

PERCENT OF PASSWORDS IDENTIFIED (CRACKED) AS NOT MEETING STRONG AUTHENTICATIONS PASSWORD (RUN NUTCRACKER IAW STANDING CONOP)

-----  
 T1=<8, T2=8-15, T3=15-25, T4=>25  
 -----

FXP:

CCC-41-SF INFORMATION ASSURANCE

---

2. ALL UNITS UNABLE TO PARTICIPATE IN ANY PART OF THIS EXERCISE SHOULD SUBMIT IMMEDIATE COMSPOT WITH SUMMARY OF DEFICIENCIES.//  
***Downgrading instructions in accordance with SECNAV M5510.36 (June 2006).***

## DRILL PACKAGE SIERRA - GBS

1. PROVIDED IS THE STANDING PRE-EX (C4I PKG SIERRA) FOR GBS MONITORING. THE CRITERIA FOR MEASURING EFFECTIVENESS AND BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

- A. EXERCISE: GBS MONITORING SCENARIO
- B. OSE: **Strike Group Commander**
- C. OTC: **Strike Group Commander**
- D. OCE: (PRI) USS **CV/CVN, LHA/LHD** (SEC) **USS CG**
- G. PARTICIPANTS: **Strike Group Units**
- I. TIME ZONE: ALL TIMES ARE ZULU
- J. COMEX: IAW SOE (NO NOTICE)
- JJ.FINEX: IAW SOE
- N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED
- U. COMMUNICATIONS: CHAT, MESSAGE.
  - A. COORDINATION CIRCUITS:
    - 1. PRI COORD:
    - 2. SEC COORD:
- V. INSTRUCTIONS:
  - V1. (C) PROCEDURES:
  - V2. (U) REPORTING REQUIREMENTS:

-----  
 ZZ.1 THIS EXERCISE IS DESIGNED TO TEST STRIKE GROUP ABILITY TO MEET THE FOLLOWING NTA'S.  
 NTA STANDARDS TO BE OBSERVED:

NTA 5.1.1.1.2 PROVIDE EXTERNAL COMMUNICATIONS GLOBAL BROADCAST SERVICE (GBS)

IS THE GBS MANAGER PROPERLY TRAINED IN SUBMITTING GBS MISSION REQUEST (GMR)?  
 T1=YES, T2=N/A, T3=N/A, T4=NO.

REVIEW PREVIOUS SUBMITTED GMR'S, OF THE 30 LINE ITEMS FORM, WHAT PERCENTAGE WAS COMPLETED CORRECTLY?  
 T1<=98, T2,98-95, T3<95-90, T4<90

IS THE STRIKE GROUP USING GBS PROPERLY?  
 T1=YES, T2=N/A, T3=N/A, T4=NO.

IS THE STRIKE GROUP IDENTIFYING INFORMATION REQUIREMENT PRODUCT REQUIREMENTS AND COORDINATING WITH THE INFORMATIN PROVIDER TO SATISFY THEIR REQUIREMENTS? OF THE STANDARD PRODUCTS PROVIDED FOR SG'S, HOW MANY ARE BEING UTILIZED/PLANNED TO BE UTILIZED? (I.E. TOMOHAWK, WEATHER, MAPS, IMAGERY, TELEVISION, INTEL BRIEFINGS, UAV VIDEI, TARGET UPDATES, MEDICAL INFO, SEAWITHC, SIPR, NIPR).  
 T1<=10, T2<9-8, T3<7-5, T4>5

TIME IN MINUTES TO DEMONSTRATE PROPER TUNING TO GBS TRANSPONDER USING CORRECT TELEMETY (TLE) DATA.  
T1<=10, T2<10-15, T3<15-20, T4>20

TIME IN MINUTES TO DEMONSTRATE PROPER SETUP AND RECEPTION OF CLASSIFIED PRODUCTS (I.E. JWICS DATA, INTEL)  
T1<=20, T2<20-30, T3<30-40, T4>40

TIME IN HOURS TO DEMONSTRATE PROPER SET UP AND CONFIGURATION OF KG-250 CRYPTO DEVICE ISO GBS.  
T1<=10, T2<10-20, T3<20-30, T4>30

TIME IN MINUTES TO DEMONSTRATE PROPER TUNING OF GBS SHIPBOARD DUAL ANTENNA SYSTEM.  
T1<=5, T2<5-10, T3<10-20, T4>20

DOES THE GBS MANAGER UNDERSTAND PROPER GBS OPERATIONS AND SETUP.  
T1=YES, T2=N/A, T3=N/A, T4=NO.

ABILITY OF THE GBS MANAGER TO IDENTIFY ALL PATHS WITHIN THE STRIKE GROUP TO PROCESS GBS DATA RECEIVED?  
T1=YES, T2=N/A, T3=N/A, T4=NO.

ABILITY OF GBS MANAGER ONBOARD THE FLAG SHIP TO VERIFY DISCRETIONARY ACCESS CONTROL (DAC) PROTECTION MEASURES ARE ENFORCED BY USER-ID AND PASSWORD WHEN BASED ON NEED-TO-KNOW WHEN RE-HOSTING GBS INFORMATION PRODUCTS ON LOCAL AREA NETWORKS.  
T1=YES, T2=N/A, T3=N/A, T4=NO.

ABILITY OF THE GBS MANAGER TO SETUP THE INTERGRATED RECEIVER DECODER (IRD) TO RECEIVE VIDEO FROM AN ALTERNATE TRANSPONDER.  
T1=YES, T2=N/A, T3=N/A, T4=NO.

-----  
FXP:  
CCC-25-SF SUPER HIGH FREQUENCY SATELLITE COMMUNICATIONS

2. ALL UNITS UNABLE TO PARTICIPATE IN ANY PART OF THIS EXERCISE SHOULD SUBMIT IMMEDIATE COMSPOT WITH SUMMARY OF DEFICIENCIES.//  
**Downgrading instructions in accordance with SECNAV M5510.36 (June 2006).**

**DRILL PACKAGE TANGO - (C4I JEOPARDY PUBEX)**

PROVIDED IS THE STANDING PRE-EX FOR C4I PKG TANGO C4I/INFO SYS/OPORD 6000 PUBEX. THE CRITERIA FOR MEASURING EFFECTIVENESS OF THE BASELINE STANDARDS WILL PRIMARILY BE BY USE OF NMETLS. ALL NMETLS CAN BE FOUND ON THE COMSTRKFORTRALANT OR COMSTRKFORTRAPAC CAS SITE. ALL RELATED WARFARE AREA NMETLS CAN BE FOUND ON THE **Strike Group** CAS SITE. IN ADDITION TO NMETLS, ALL UNITS WILL USE THE

FXP-3 AND SELF-OBSERVE APPLICABLE AREAS AND PROVIDE OBSERVED GRADED STATUS.

A. STANDARD PRE-EX FOR C4I PACKAGE TANGO PUBEX

A. EXERCISE: EXECUTION OF C4I PUBEX

A. EXERCISE: IA MONITORING SCENARIO

B. OSE: **Strike Group Commander**

C. OTC: **Strike Group Commander**

D. OCE: (PRI) USS **CV/CVN, LHA/LHD** (SEC) **USS CG**

G. PARTICIPANTS: **Strike Group Units**

I. TIME ZONE: ALL TIMES ARE ZULU

J. COMEX: IAW SOE (NO NOTICE)

JJ.FINEX: IAW SOE

N. AREA OF EXERCISE: IAW CURRENT TASKING AS ASSIGNED

U. COMMUNICATIONS: CHAT, MESSAGE.

A. COORDINATION CIRCUITS:

1. PRI COORD:

2. SEC COORD:

V. INSTRUCTIONS:

V1. ALL UNITS MUST BE PREPARED TO ACTIVATE DESIGNATED CIRCUIT LINE NUMBER UPON REQUEST VIA COMSPOT AS DIRECTED BY CCS.

V2. CCS WILL CONDUCT ROLL CALL ON PRIMARY COMM COORD CIRCUIT AS ASSIGNED. EACH UNIT WILL INITIATE CALL UP TO THE CONTROL SHIP ADVISING RECEIPT AND READABILITY OF ROLL CALL.

-----  
- GOAL CONDUCT C4I JEOPARDY PUBEX VIA COMM COORD.  
-----

- **USS** \_\_\_\_\_ WILL ACT AS ALEX TREBEK  
-----

- C4I JEOPARDY (PUBEX) REFERENCES NTP 4 (F)  
**Strike Group Commander** OPORD 6000 (LOCATED ON CAS II SITE)  
NWP 6-01 (REV A)  
NTP 3 SUPP-1 (L)  
EKMS 1  
-----

- **USS** \_\_\_\_\_ (ALEX TREBEK) WILL ASK A TOTAL OF 20 QUESTIONS IN A ROUND ROBIN FASHION TO ALL PARTICIPANTS. EACH SHIP HAS TWO MINUTES TO PROVIDE CORRECT ANSWER AFTER ROGER OUT.

- EACH QUESTION ANSWERED CORRECTLY IS WORTH 2 POINTS EACH AND EACH INCORRECT ANSWER WILL BE A DEDUCTION OF 2 POINTS. IF UNIT UNABLE TO ANSWER THE QUESTION IT WILL THEN BE FORWARDED OVER TO THE OTHER PARTICIPANT FOR THE ANSWER AND THE POINTS.

- ALL ANSWERS WILL BE PROVIDED ALONG WITH PAGE NUMBER AND

PARAGRAPH. CONDUCT COMM CHECK 30 MIN PRIOR TO EVENT COMEX ON COMM COORD AS ASSIGNED IAW SOE.

-----  
V.3. PUBEX WILL BE CONDUCTED FOR THE DAY AND NIGHT WATCHTEAMS

V.4. OCE WILL GENERATE COMSPOT DETAILING PUBEX UPON FINEX AND PROVIDE GRADE STANDARDS AND MEASURES OF EFFECTIVENESS.

RESULTS TO BE POSTED ON **Strike Group** CAS II: **indicate IP address.**//

**Downgrading instructions in accordance with SECNAV M5510.36 (June 2006).**

**THIS PAGE INTENTIONALLY BLANK**