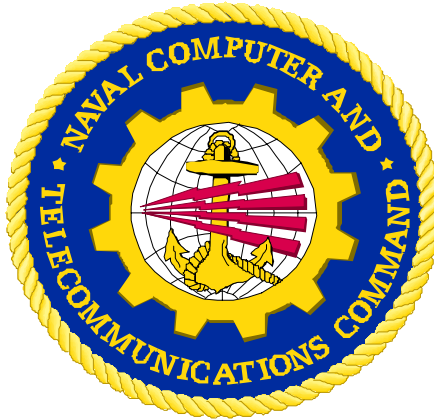


**NAVAL TELECOMMUNICATIONS PROCEDURES**  
**DEFENSE MESSAGE SYSTEM**  
**LOCAL OPERATIONS AND NETWORK MANAGEMENT POLICIES AND**  
**PROCEDURES**



**NTP 22**

**NAVAL COMPUTER AND TELECOMMUNICATIONS COMMAND**  
**NEBRASKA AVENUE COMPLEX**  
**4234 SEMINARY DRIVE N.W. SUITE 19122**  
**WASHINGTON, D.C. 20394-5460**

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

**07 September 2000**

**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  
NAVAL COMPUTER AND TELECOMMUNICATIONS COMMAND  
NEBRASKA AVENUE COMPLEX  
4234 SEMINARY DRIVE N.W. SUITE 19122  
WASHINGTON, D.C. 20394-5460

LETTER OF PROMULGATION

1. The Commander, Naval Computer and Telecommunications Command (COMNAVCOMTELCOM) directed development of NTP 22, Defense Message System (DMS) Local Operations and Network Management Policies and Procedures, and promulgated it for use by U.S. Navy, U.S. Marine Corps, and U.S. Coast Guard activities. NTP 22 provides policies and procedures for the operation and management of Department of the Navy (DoN) and U.S. Coast Guard DMS site-level Area Control Centers (ACC), Local Control Centers (LCC), and Remote Service Sites (RSS).
2. NTP 22 is an UNCLASSIFIED, non-registered publication.
3. NTP 22 is **EFFECTIVE UPON RECEIPT** and will co-exist with NTP 3(J) until the Department of the Navy (DoN) transitions from DTH legacy systems to full DMS operational capability.
4. COMNAVCOMTELCOM grants permission for authorized holders to copy or extract information from this publication.
5. Personnel may carry this publication or extracts thereof in aircraft for use therein.
6. Commands should address correspondence concerning this publication via the normal military chain of command to Commander, Naval Computer and Telecommunications Command, Nebraska Avenue Complex, 4234 Seminary Drive N. W. Suite 19122, Washington, D.C. 20394-5460.
7. The Secretary of the Navy (SECNAV) has approved this publication in accordance with Instruction 5600.16.



G. F. ALLEN  
Colonel

United States Marine Corps  
Division Head, Strategic  
Planning Division  
Command, Control, Communications,  
And Computer



C.G. COOPER, III  
Captain, U.S. Navy  
Commander, Naval Computer and  
Telecommunications Command



TABLE OF CONTENTS

Letter of Promulgation .....	I
Record of Changes and Corrections .....	II
Table of Contents .....	III
Table of Figures .....	VIII
List of Tables .....	IX
List of Appendices .....	IX

CHAPTER 1INTRODUCTION

101	Purpose .....	1-1
102	Scope .....	1-1
103	Background .....	1-1
104	Direction .....	1-2
105	References .....	1-2

CHAPTER 2DON DMS ARCHITECTURE

201	General .....	2-1
202	DoN DMS Architecture .....	2-1
203	DMS Component Descriptions .....	2-4
203.1	DMS Client or User Agent .....	2-4
203.2	DMS Fortezza Card .....	2-4
203.3	Groupware Server (GWS) .....	2-4
203.4	Message Store (MS) .....	2-4
203.5	Defense Message Dissemination System (DMDS) .....	2-5
203.6	Profiling User Agent (PUA) .....	2-5
203.7	High Assurance Guard (HAG) .....	2-5
203.8	Local Message Transfer Agent (LMTA) .....	2-6
203.9	Backbone Message Transfer Agent (BMTA) .....	2-6
203.10	Directory Systems Agent (DSA) .....	2-6
203.11	Multi-Function Interpreter (MFI) .....	2-6
203.12	Mail List Agent (MLA) .....	2-7
203.13	Service Management System (SMS) .....	2-7
203.14	Certification Authority Workstation (CAW) .....	2-7

**CHAPTER 3****DMS MANAGEMENT STRUCTURE**

301	General.....	3-1
302	Global Network Operations and Security Center (GNOSC)	3-1
303	Regional Network Operations and Security Center (RNOSC).	
	.....	3-5
304	Navy Local Network Operations and Security Center (Navy LNOSC)	3-6
304.1	Area Control Center.....	3-6
304.2	Local Control Center.....	3-7
304.3	Remote Service Center.....	3-7
305	General Navy LNOSC Responsibilities.....	3-7

**CHAPTER 4****OPERATIONAL ROLES AND RESPONSIBILITIES**

401	General.....	4-1
402	Defense Information Systems Agency (DISA).....	4-1
402.1	DISA DMS Global System Manager (GSM).....	4-1
402.2	DISA DMS Regional System Manager (RSM).....	4-1
403	Navy Management Roles.....	4-2
403.1	Commander Naval Computer and Telecommunications Command (COMNAVCOMTELCOM).....	4-2
403.2	Navy Global System Manager (Navy GSM).....	4-2
403.3	Navy Area/Local System Manager (ASM/LSM).....	4-2
404	Navy Mandatory Roles.....	4-3
404.1	DoN Sub-Registration Authority (SRA).....	4-3
404.2	Organizational Registration Authority (ORA).....	4-6
404.3	Organizational System Administrator (OSA).....	4-7
404.4	Organizational Security Officer (OSO).....	4-9
404.5	Certification Authority (CA).....	4-10
404.6	Mail List Manager (MLM).....	4-11
404.7	Navy LNOSC Help Desk (HD) Specialist.....	4-12
404.8	Navy Area or Local System Manager (ASM or LSM).....	4-13
404.9	Operations Manager (OM).....	4-14
405	U.S. Marine Corps Management Roles.....	4-14

**CHAPTER 5****DON DMS OPERATIONAL ROLES AND ACCOUNTS**

501	General.....	5-1
502	Operations Accounts.....	5-1
503	Registration Criteria for Navy Role Names.....	5-2
503.1	Symbols and Capitalization Rules.....	5-2
503.2	Standard Role Names.....	5-3
503.3	Certification Authorities.....	5-4
503.4	Registration Authorities.....	5-4
503.5	Navy Global System Manager.....	5-4

503.6	Navy DMS Operations Manager.....	5-4
503.7	Area Control Center Names.....	5-4
503.8	Local Control Center.....	5-5
503.9	Remote Server Site.....	5-5
503.10	Mandatory Role Names for Management Centers.....	5-5
503.11	Optional Role Names for Management Centers.....	5-6
503.12	Mandatory Organizational Roles.....	5-6
504	USMC Registration Criteria.....	5-6

## CHAPTER 6

### NAVY LNOSC OPERATING PROCEDURES

601	General.....	6-1
602	RADAY Change Procedures.....	6-1
602.1	Reports.....	6-1
602.2	Audit Collection.....	6-1
602.3	System Backups.....	6-1
602.4	Help Desk Logs.....	6-1
602.5	Operations Message Files.....	6-1
603	Shift Change Procedures.....	6-1

## CHAPTER 7

### INTERIM PROCEDURES

701	General.....	7-1
702	Interim Procedure Notice (IPN).....	7-1
703	Interim Procedure Description.....	7-1
704	Finalizing an Interim Procedure.....	7-2

## CHAPTER 8

### TROUBLE TICKET PROCEDURES

801	General.....	8-1
802	Trouble Tickets.....	8-1
803	Trouble Ticket Priority and User Impact.....	8-1
804	Navy LNOSC Trouble Ticket Procedures.....	8-1
805	Escalated Trouble Ticket Procedures.....	8-2

## CHAPTER 9

### MESSAGE TRACE PROCEDURES

901	General.....	9-1
902	Message Trace Procedure.....	9-1
903	Thresholds for Message Trace Initiation.....	9-2
904	Lost Message.....	9-3
905	Record Retention.....	9-3
906	Speed of Service Considerations.....	9-5
907	Message Trace Process Diagram.....	9-5

908	Message Trace Scenario Example.....	9-9
-----	-------------------------------------	-----

## CHAPTER 10

### SOFTWARE PATCH PROCEDURES

1001	General.....	10-1
1002	Policy.....	10-1
1003	Evaluation and Testing.....	10-1
1004	Field Engineering Notice (FEN).....	10-1
1005	Defense Information Infrastructure (DII) Asset Distribution System (DADS) Posting.....	10-1
1006	Patch Notification.....	10-2
1007	DoN Distribution Requirements.....	10-2
1008	Distribution of Large Patches.....	10-2
1009	Navy LNOSC Patch Installation.....	10-2
1010	Patch Installation Problem Resolution.....	10-3
1011	Reporting.....	10-3
1011.1	Navy LNOSC Reporting.....	10-3
1011.2	USMC LCC Reporting.....	10-3
1011.3	RNOSC Reporting.....	10-3
1012	Overdue Patch Installation.....	10-3
1013	USMC Patch Installation.....	10-4

## CHAPTER 11

### SYSTEM UPGRADE PROCEDURES

1101	General.....	11-1
1102	Scope.....	11-1
1103	Overview.....	11-1
1103.1	DMS Product Releases.....	11-1
1103.2	DMS Implementation Strategy and Plan (ISP) for DMS Releases.....	11-1
1104	Operational Impact.....	11-2
1105	Transition Procedures.....	11-2
1106	Transition Schedule.....	11-2
1107	GSM Authorization to Install.....	11-2
1108	Software Distribution.....	11-3
1109	Upgrade Status Ticket.....	11-3
1110	Site Specific Upgrade Procedures.....	11-4
1110.1	RNOSC, Regional Node, and DTH Upgrade Procedures....	11-4
1110.2	Beta Test Site Upgrade Procedures.....	11-4
1111	Upgrade Procedures.....	11-5
1112	System Upgrade Reporting.....	11-6
1113	DMS Upgrade Completion.....	11-6
1114	DMS Release Testing.....	11-6
1114.1	DMS Product Testing.....	11-6
1114.2	DMS Integration Testing.....	11-7
1114.3	DMS Verification Testing.....	11-7
1114.4	Navy Verification Testing.....	11-8

**CHAPTER 12****DMS REPORTING PROCEDURES**

1201	General.....	12-1
1202	System Monitoring.....	12-1
1203	Navy LNOSC Automated System Management Reporting....	12-1
1204	Activation of the Reports.....	12-1
1205	System Status Report.....	12-1
1205.1	Requesting the System Status Report.....	12-2
1205.2	Customizing the System Status Report.....	12-2
1206	Cumulative Statistics Report (CumStat).....	12-5
1206.1	Activating the Cumulative Statistics Report.....	12-5
1206.2	Customizing the Cumulative Statistics Report.....	12-5
1207	Non-automated Reporting Requirements.....	12-8
1207.1	Daily Navy LNOSC Summary Report.....	12-8
1207.2	Daily Navy LNOSC System Performance Report.....	12-8
1208	Routine or Historical Operations.....	12-8
1209	DMS Asset and Inventory Control.....	12-10
1210	Report Retention.....	12-10

**CHAPTER 13****CONFIGURATION CHANGE PROCEDURES**

1301	General.....	13-1
1302	Scope.....	13-1
1303	Design Validation Team (DVT).....	13-1
1304	Design Review Order and Precedence.....	13-2
1305	Detailed Designs.....	13-3
1306	Changes Involving the Backbone Infrastructure.....	13-3
1306.1	Routine Change Procedures.....	13-3
1306.2	Emergency Change Procedures.....	13-5
1307	Changes Not Involving the Backbone Infrastructure..	13-5

**CHAPTER 14****HIGH ASSURANCE GUARD PROCEDURES**

1401	General.....	14-1
1402	HAG Placement.....	14-1
1403	HAG Keyword Criteria.....	14-2

**CHAPTER 15****FIREWALL PROCEDURES**

1501	General.....	15-1
1502	Firewall Description.....	15-1
1503	Local Firewall Implementation.....	15-1
1504	Policy.....	15-1
1505	Protocols.....	15-2



1506	Protocol Guidance.....	15-2
------	------------------------	------

## CHAPTER 16

### SERVICE INTERRUPTION PROCEDURES

1601	General.....	16-1
1602	Part-time and Dial-in Users.....	16-1
1603	Service Interruptions.....	16-1
1603.1	Authorized Outage.....	16-1
1603.2	Unauthorized Outage.....	16-2
1604	Outage Reporting.....	16-2
1605	Planned Service Interruption at the Navy LNOSC.....	16-2
1606	Planned Service Interruption at the User Location...	16-3
1607	Response to Authorized Interruption Request.....	16-3
1608	Preliminary and Final Concurrence Actions.....	16-3
1609	Alternate Route Requirement.....	16-4
1610	Planned Service Interruption at the RNOSC.....	16-4
1611	Emergency Service Interruptions.....	16-6
1611.1	Planned Outage at the User Location.....	16-6
1611.2	Planned Outage at the Navy LNOSC.....	16-6
1612	Trouble Ticket Reporting by the Navy LNOSC.....	16-6
1613	Unplanned Outage.....	16-6
1613.1	Navy LNOSC Unplanned Outage.....	16-7
1613.2	User Unplanned Outage.....	16-7
1614	Restoration of Service.....	16-8
1614.1	Restoration of Service to a User.....	16-8
1614.2	Restoration of Service of a Navy LNOSC.....	16-8

## CHAPTER 17

### NAVY LNOSC AND USMC/USCG LCC BACKUP PROCEDURES

1701	General.....	17-1
1702	Component System Backup Procedures.....	17-1
1702.1	LNOSC and USMC/USCG Windows NT Backup Procedures...	17-1
1702.2	LNSOC and USMC/USCG UNIX Backup Procedures.....	17-2
1703	Restoration of a Component Using Backups.....	17-3

### TABLE OF FIGURES

Figure 2-1	Navy Notional DMS Architecture.....	2-2
Figure 2-2	USMC DMS Architecture.....	2-3
Figure 3-1	DMS Management Structure.....	3-2
Figure 3-2	Navy Management Structure.....	3-3
Figure 3-3	USMC Management Structure.....	3-4
Figure 8-1	Problem Reporting Process Flowchart.....	8-4
Figure 8-2	ACC NCTAMS LANT Norfolk VA Reporting and Management Structure.....	8-8
Figure 8-3	ACC NCTAMS EURCENT Naples Italy Reporting and Management Structure.....	8-9
Figure 8-4	ACC NCTAMS PAC Honolulu HI Reporting and Management Structure.....	8-10

Figure 8-5	ACC NAVCOMTELSTA San Diego CA Reporting and Management Structure.....	8-10
Figure 9-1	Diary Section from Message Trace.....	9-5
Figure 9-2	DMS Message Trace Flowchart.....	9-6
Figure 9-3	Message from Originator Organization to LNOSC...	9-11
Figure 9-4	Message from the LNOSC to RNOSC-C.....	9-12
Figure 9-5	Message from RNOSC-C to RNOSC-E.....	9-13
Figure 9-6	Message from RNOSC-E to Recipient's LNOSC.....	9-14
Figure 9-7	Message from Recipient's LNOSC to All Concerned.	9-15
Figure 12-1	System Status Report Request Window.....	12-3
Figure 12-2	System Status Report (Partial).....	12-4
Figure 12-3	Cumulative Statistics Report Request Window....	12-6
Figure 12-4	Cumulative Statistics Report (Partial).....	12-7
Figure 13-1	Detailed Design Change Process.....	13-6
Figure 15-1	Common Local Network Firewall Implementation....	15-4
Figure 16-1	Authorized Service Interruption Request Ticket..	16-5

#### LIST OF TABLES

Table 3-1	RNOSC Designations and Areas of Responsibility....	3-6
Table 5-1	Standard Management Role Names.....	5-3
Table 8-1	Trouble Ticket Priority Table.....	8-5
Table 8-2	Trouble Ticket Preparation Form.....	8-6
Table 9-1	Message Trace Thresholds.....	9-3
Table 15-1	Firewall Protocol.....	15-5

#### LIST OF APPENDICES

Appendix A	Acronyms.....	A-1
Appendix B	Glossary of Terms.....	B-1
Appendix C	DoN LNOSC Locations.....	C-1
Appendix D	DMS Management Operational Accounts.....	D-1

**CHAPTER 1****INTRODUCTION****101. Purpose**

The Naval Telecommunications Procedures (NTP) 22, Defense Message System (DMS) Local Management Policies and Procedures, provides policies and procedures governing the management and operation of the Department of the Navy (DoN) segment of the DMS, and the operation of DoN and U.S. Coast Guard (USCG) DMS Area Control Centers (ACC), Local Control Centers (LCC), and Remote Service Sites (RSS). NTP 22 applies to U.S. Navy, U.S. Marine Corps (USMC), USCG, and other activities served by the DoN telecommunications facilities.

**102. Scope**

NTP 22 provides standard policies and procedures for the operation and management of all Navy and USCG control centers (ACC'S, LCC'S, and RSS'S) and USMC LCC'S (where common operating procedures apply, the term "site" will be used to describe Navy and USCG ACC'S, LCC'S, and RSS'S and USMC LCC'S). NTP 22 also provides a comprehensive view of those centers and their relationship to other components within the DMS architecture. NTP 22 is, therefore, an informative source for all DoN echelons authorized to utilize the DMS. The policies and procedures described in this document support the targeted capabilities of product releases 2.1 and 2.2. This document will co-exist with the NTP 3 (series) procedures during the transition from the DTH legacy system to DMS. During this transitional period, the policies and procedures outlined herein will complement the instructions outlined in the NTP 3 (series) procedures and other DoN DMS publications. The Commander, Naval Computer and Telecommunications Command (COMNAVCOMTELCOM) will announce changes to this publication via message and disseminate changes via the COMNAVCOMTELCOM Home Page at "[www.nctc.navy.mil](http://www.nctc.navy.mil)".

**103. Background**

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD C3I) has designated DMS as the messaging system of record for the Department of Defense (DoD) and supporting agencies. DMS is based on Joint Staff approved requirements as defined in the Multi-command Required Operational Capability (MROC 3-88). It is a flexible, Commercial-Off-The-Shelf (COTS)-based, network-centric application layer system that provides multi-media messaging and directory services capable of taking advantage of the flexible and expandable underlying Defense Information Infrastructure (DII) network and security services. The DoN will deploy DMS to all U.S. Navy, USMC, USCG activities, and other Service or Agency users serviced by the DoN's DMS infrastructure.

#### 104. Direction

The DMS consists of all hardware, software, procedures, standards, facilities, and personnel used to exchange electronic messages between organizations and individuals in the DoD. Services and Agencies manage and operate the DMS as a collective resource for the DoD and as a Joint Service system in accordance with priorities established by the Chairman, Joint Chiefs of Staff. The Naval Computer and Telecommunications Command (NAVCOMTELCOM) provides policy, procedures, and direction for Navy Local Network Operations and Security Centers (LNOSC) that inter-operate and interface with the global DMS infrastructure. The LNOSC acronym is a generic reference used interchangeably throughout the document to refer to Navy Control Centers (Area Control Centers (ACC), Local Control Centers (LCC), or Remote Server Sites (RSS)). This document will use the ACC, LCC, or RSS abbreviation when it is important to distinguish between the type of control center.

Similarly, USMC LCC'S will be under the direction of the DMS Central Operations Center (DCOC), which is a part of the Marine Corps Information and Technology and Network Operations Center (MITNOC) at Quantico, VA.

Unless indicated otherwise, the duties and responsibilities described for the Navy LNOSC also apply to the USMC LCC'S. NTP 22 is applicable to DoN and USMC activities and to any other service or agency served by the DoN.

The policies, procedures, and operational guidelines outlined herein are for individuals and organizations that use or derive DMS services from DoN facilities. Within DoN, the procedures and policies outlined in this document shall supersede and take precedence over other Service and Agency DMS publications and shall be considered as the authoritative source for DMS policies and procedures for DoN DMS facilities and operating environments.

#### 105. References

The following references amplify and supplement policies and procedures outlined herein. The latest versions of the following referenced documents are available on the COMNAVCOMTELCOM Web site, "[www.nctc.navy.mil](http://www.nctc.navy.mil)."

a. **ACP 117 CAN-U.S. SUPP-1 (Allied Communications Publication 117, Allied Routing Indicator Book, Canada-United States Supplement 1)** - This document contains the procedures that govern submission of requests for routing by activities having geographic locations and mobile units operating fixed-plant DTH terminals. This document is not a Plain Language Address (PLA) verification tool and will be used only as a routing reference guide.

b. **ACP 120 (Allied Communications Publication 120, Common Security Protocol (CSP))** - The requirement for secure electronic mail and secure messaging resulted in the development of a security protocol to be used with the Consultative Committee International Telegraph (CCITT) X.400 Message Handling System. Developers called this protocol the Message Security Protocol (MSP). In order to commercialize MSP as a common protocol for wider use, the original document (SDN.701) has been rewritten and renamed ACP 120. While this specification is oriented toward use within an X.400 Message Handling System (MHS), CSP may also function as a secure message and protocol encapsulation facility with other distributed computing environments, such as directory access and key material distribution.

c. **ACP 121 U.S. SUPP-1 (Allied Communications Publication 121, United States Supplement 1)** - This document provides instructions for communications and operations associated with the use of the DoD record message system. It contains information, such as the description of message release procedures, pertinent during normal operations. This publication also contains information related to special considerations such as the implementation of MINIMIZE conditions.

d. **ACP 123 Edition A (Allied Communications Publication 123)** - This document outlines Common Messaging Strategy and Procedures and describes all services, procedures, and protocols that support Allied military X.400 messaging environments.

e. **ACP 123 U.S. SUPP-1 (Allied Communications Publication 123, United States Supplement 1)** - This document defines U.S. national general policies and procedures for DMS military messaging. This document supplements guidance outlined in ACP 123 and identifies numerous technical and procedural issues that require further definition and refinement at the DoD Service and Agency level.

f. **ACP 133 (Allied Communications Publication 133, Common Directory Services and Procedures)** - This document defines the directory services, architecture, protocols, schema, policies, and procedures to support Allied communications, including Military Message Handling System (MMHS) services based on ACP 123, in both the strategic and tactical environments.

g. **CMS-9, Director Communications Security Material Systems (DCMS); DMS Communications Security** - This document outlines policy and procedures that define the overall requirements and implementation guidance, including details of handling, inventory, and reporting procedures for Fortezza cards. Fortezza is a component of the MISSI and is used in conjunction with other MISSI components.

h. **Department of the Navy (DoN) Computer Incident Response Guidebook, NAVSO-5239-19** - This incident response guidebook provides procedures to recover from computer security incidents.

i. **Department of the Navy (DoN) Information Systems Security Manager (ISSM) Guidebook, Module 04, NAVSO-5239-04** - This guidebook provides guidance and direction to ISSM'S in implementing and managing overall INFOSEC programs. Specifically, it provides the responsibilities of the ISSM and provides instructions for implementing these responsibilities.

j. **Department of the Navy (DoN) Information Systems Security Officer (ISSO) Guidebook, Module 07, NAVSO-5239-07** - This guidebook provides guidance and direction to ISSO'S in implementing and managing overall INFOSEC programs. Specifically, it provides the responsibilities of the ISSO and provides instructions for implementing these responsibilities.

k. **Department of the Navy (DoN) Network Security Officer (NSO) Guidebook, Module 08, NAVSO-5239-08** - This guidebook provides guidance and direction to NSO'S in implementing and managing overall INFOSEC programs. Specifically, it provides the responsibilities of the NSO and provides instructions for implementing these responsibilities.

l. **Defense Information Systems Agency (DISA) DMS Site Commissioning Document** - This document outlines policies and procedures for testing, activating, and commissioning new DMS sites.

m. **DISAC 310-M70-87 (Defense Message System Operational Policies and Procedures)** - This document contains high level DISA policies and procedures for the operation and management of the DMS.

n. **DISAC 310-M70-zz (number pending) (DMS RNOSC, Regional Node, DTH, and ACC/LCC Operations)** - This document contains high level DISA procedures for the standardization of operations at the DMS operations and management centers and for DMS interface operations at the DMS Transition Hubs (DTH).

o. **DMS Firewall Configuration Guidance** - This document provides firewall configuration guidance and information for reference and use by Services and Agencies when implementing DMS.

p. **DMS Organizational Messaging Concept of Operations (CONOPS)** - This DISA document outlines operational concepts and procedures for deploying and operating DMS components. The document describes how DMS works operationally, explains DMS capability options and how to use them, including how DMS and DTH users will exchange organizational messages during DMS implementation and DTH phase-out. Appendices D and E outline concepts and procedures relating specifically to the U.S. Navy, the USMC, and the USCG.

q. **DMS System Design Architecture Release Current Version** - This document describes the capabilities and functionality of DMS

components and outlines DMS architectural strategies for deploying and operating DMS components.

r. **DMS System Manual** - This document provides assistance for implementation, daily operation, and maintenance of the DMS system environment. The System Manual is not a Standard Operations Procedures (SOP) or operations policy manual.

s. **DoD 5200.28 Security Requirements for Automated Information Systems (AIS'S); w/Ind, ASB-IS-A** - This document provides mandatory minimum DOD-wide Automated Information System (AIS) Security Requirements.

t. **Draft Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)** - This document provides policy and procedures for Certification and Accreditation (C&A) of Information Technology (IT), including automated information systems, networks, and sites in the DOD.

u. **Naval Warfare Publications (NWP'S) - NWP 6-01 (Basic Operational Communications Doctrine)** - This document provides basic doctrine and amplifying information related to the operation of the Naval Computer and Telecommunications System (NCTS). The NWP 1-03 (Joint Reporting System) series includes instructions for the preparation of required operations reports. This series contains amplifying information describing data fields used in special-purpose message formats (e.g., Casualty Report (CASREP), Movement Report (MOVREP), and the Status of Resource and Training System (SORTS) report).

v. **NTP 21(A)** - Naval Telecommunications Procedure 21(A) is the policy and procedures document for the preparation and electronic delivery of DMS organizational messages.

w. **NTP 21 SUPP-1** - Naval Telecommunications Procedures 21 SUPP-1 is the policy and procedures document for the registration of organizational users, individual users, Originator/Recipient (O/R) Addresses, Mail Lists, DMS components, and technical objects.

x. **OPNAVINST 5239.1 (DoN Automatic Data Processing (ADP) Security Program)** - This document describes requirements associated with the preparation of electronic media used to prepare, transfer, and store record messages. It contains procedures for formatting and electronic labeling of new, blank diskettes. It also contains procedures for clearing and reformatting diskettes for reuse.

y. **SECNAVINST 5210.11(D) (DoN File Maintenance Procedures and Standard Subject Identification Code (SSIC) Index)** - This document lists all authorized SSIC'S. APP-3 North Atlantic Treaty Organization (NATO) Subject Indicator System (NASIS) is the corresponding publication listing all authorized NATO Subject Indicator Codes (SIC).

z. **Secret Internet Protocol Router Network (SIPRNET) Dial-In User Guide** - This document serves as a handbook for SIPRNET dial-in users on all aspects of gaining access and using the dial-in service. It identifies requirements, including hardware, user accounts, hardware configuration, establishing connections, and security (i.e., documentation and do's and don'ts). The dial-in service is composed of various hardware and software components. The hardware components consist of the local terminal(s), remote hosts, Secure Telephone Unit III(STU-III), Secure Telephone Equipment (STE), key material, Communication Servers (CS), and routers. The software components include protocols, modem applications, and secure telephone devices (STE and STU-III key material).

aa. **X.400 (ITU-TSS Data Communications Networks, Message Handling Systems (MHS) Recommendations)** - This document contains international recommendations for the operation of message handling systems.

bb. **X.500 (ITU-TSS Data Communications Networks, Directory Recommendations)** - This document contains international recommendations for the directory structure and access.



**CHAPTER 2****DON DMS ARCHITECTURE****201. General**

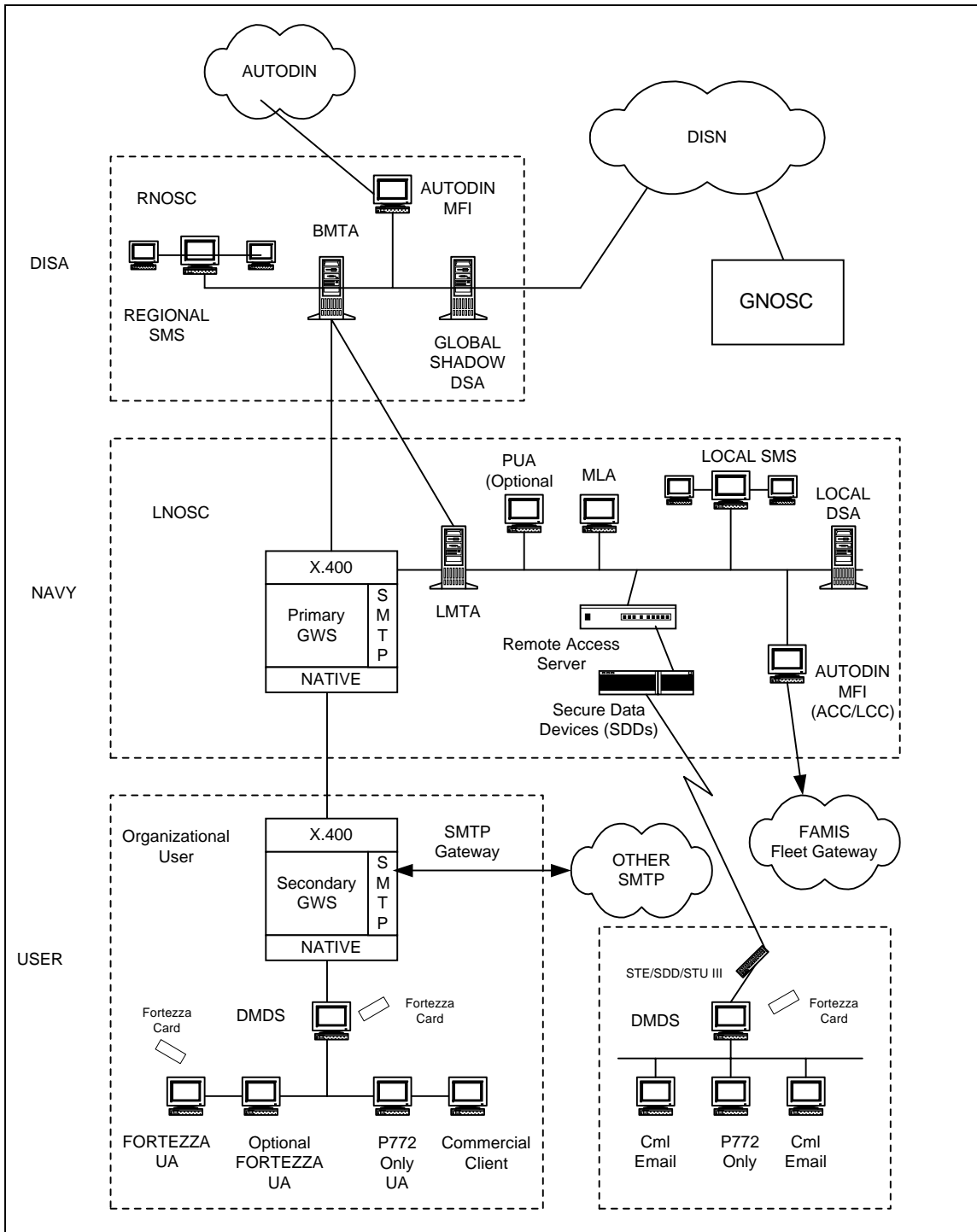
This chapter describes the DMS architecture and components for Navy LNOSC operations and management personnel. While this description is general, the chapter provides sufficient information about the various components to enable the reader to understand the use of each component and the way in which they work together in DMS.

**202. DoN DMS Architecture**

DoN DMS architecture is comprised of messaging, directory, and service management components that provide secure integrated writer-to-reader messaging for DoN users.

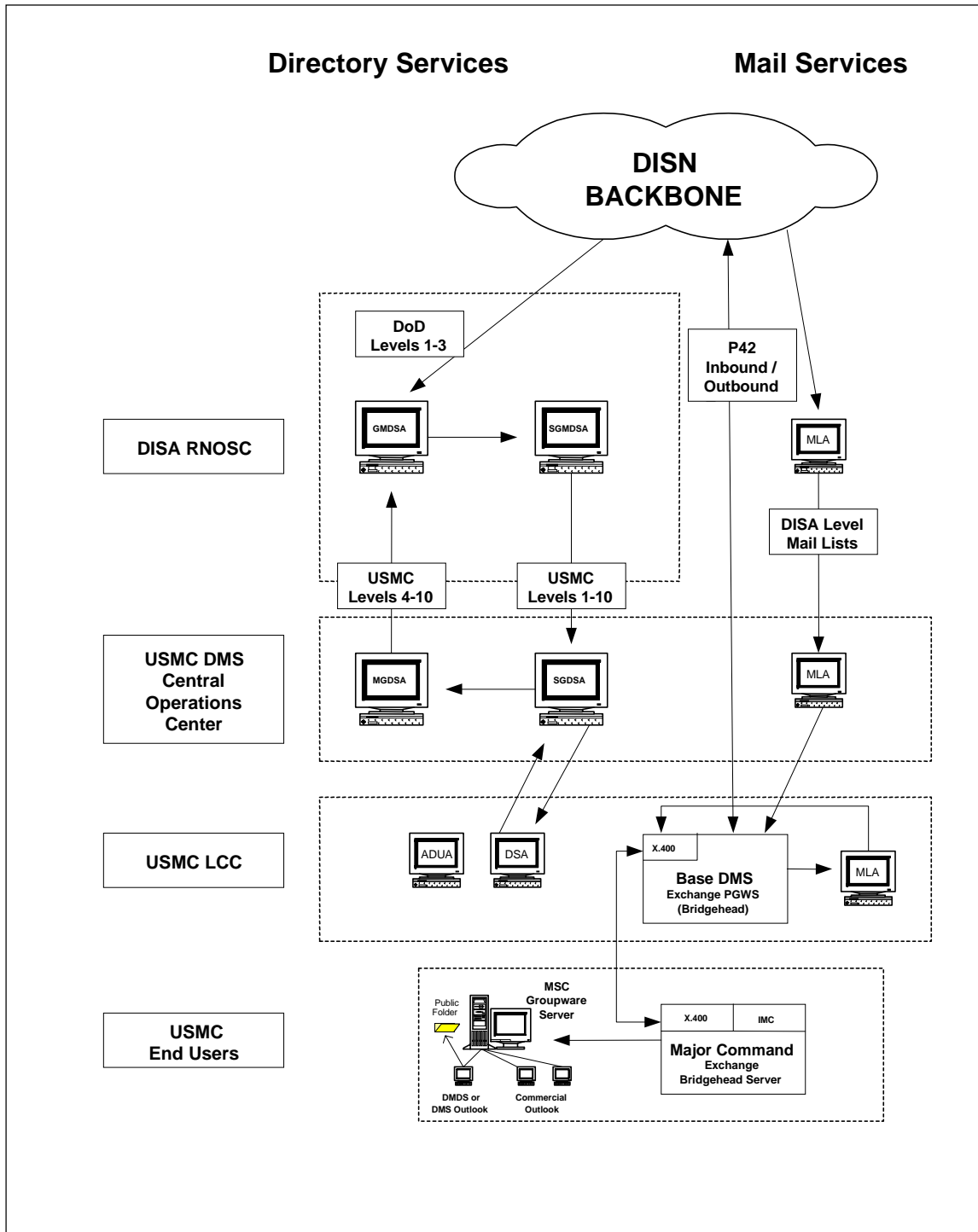
The Navy DMS architecture supports multiple DMS implementation strategies. Navy commands and organizations are permitted to select the DMS implementation options that best suit their operational requirements. The available implementation options range from a single DMS client supporting one or more organizations to large-scale multi DMS component based solutions at large command and major claimant sites. A full explanation of this flexible implementation strategy and site configuration options is outlined in the Navy DMS Organizational Messaging Concept of Operations (CONOPS). The Navy DMS architecture is depicted in Figure 2-1.

Figure 2-2 depicts the USMC architecture. USMC commands will implement an organizational messaging concept where outbound messages will be released from the desktop by designated releasers while inbound traffic will be delivered to the organization. Based on the organization's established procedures, messages will be unencrypted by an automated or manual process, profiled, and placed in folders or mailboxes. The USMC DMS Organizational Messaging CONOPS contains a full explanation of the operational configuration.



**Figure 2-1**

**Navy Notional DMS Architecture**



**Figure 2-2**

**USMC DMS Architecture**

### **203. DMS Component Descriptions**

This section provides a brief description of each of the DMS components.

#### **203.1 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.

#### **203.2 DMS Fortezza Card**

The Fortezza card, a MISSI product, is a Personal Computer Memory Card International Association (PCMCIA) card that provides high assurance cryptographic services to DMS applications. These cards are rugged, credit card-size peripherals that add security and authentication capabilities to computers. The Fortezza card stores a user's private keys (Key Exchange Algorithm (KEA) key and Digital Signature Standard (DSS) key) and public certificate. The private keys and public certificates are used to support digital signature operations and message encryption.

#### **203.3 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.

#### **203.4 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.

### **203.5 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.

### **203.6 Profiling User Agent (PUA)**

The PUA provides an organization with the capability for onward delivery of incoming messages. Messages routed to the PUA contain the addressing and security information that is associated with one or more organizations supported by the PUA. Once the message is received at the PUA, it is opened using the associated organization's Fortezza identity, profiled in accordance with the organization's profile settings, and disseminated to recipients identified in the profile settings. The organization can also configure the PUA to profile and distribute out-bound messages on behalf of the organization.

### **203.7 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:

- a. The organization has digitally signed and encrypted messages exchanged between NIPRNET and SIPRNET domains.
- b. Message originators and recipients are authorized to exchange messages between the DMS NIPRNET and SIPRNET messaging domains.
- c. All exchanged messages via the HAG are appropriately marked as unclassified.
- d. Messages exchanged between the two messaging domains do not include file attachment(s).

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.

### **203.8 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), Multi-Function 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.

### **203.9 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.

### **203.10 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.

### **203.11 Multi-Function Interpreter (MFI)**

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.

**203.12 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. Engineering Field Activities (EFA) typically install the MLA component at Navy LNOSC'S, major claimant sites, or USMC DCOC.

**203.13 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.

**203.14 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.

**CHAPTER 3****DMS MANAGEMENT STRUCTURE****301. General**

This chapter provides a description and understanding of the overall management of the DMS. It also includes a brief description of the Navy LNOSC and the roles of the Area System Manager (ASM) and the Local System Manager (LSM). Figure 3-1 shows the overall management structure of the DMS. Figure 3-2 shows the general management structure of the Navy. Figure 3-3 shows the general management structure of the USMC.

**302. Global Network Operations and Security Center (GNOSC)**

The GNOSC, located at DISA Headquarters in Arlington, VA, performs executive management oversight and technical direction of the DMS. The GNOSC supports the Global System Manager (GSM) and the global staff elements by providing performance status information and such other reports as the staff may require. GNOSC managers are capable of monitoring DMS elements of the RNOSC'S, receiving messaging service performance reports, and maintaining a global view of the DMS. The GNOSC does not normally exercise a direct management function. Additional duties of the GNOSC are:

- a. Exercising oversight of the RNOSC'S.
- b. Coordinating traffic management between Regions.
- c. Coordinating inter-regional issues.
- d. Generating statistical and command reports.
- e. Coordinating system reconfiguration when more than one region is involved.
- f. Acting as arbitrator in cases where lower level management responsibilities are unclear.
- g. Preparing a SOP for GNOSC operations.



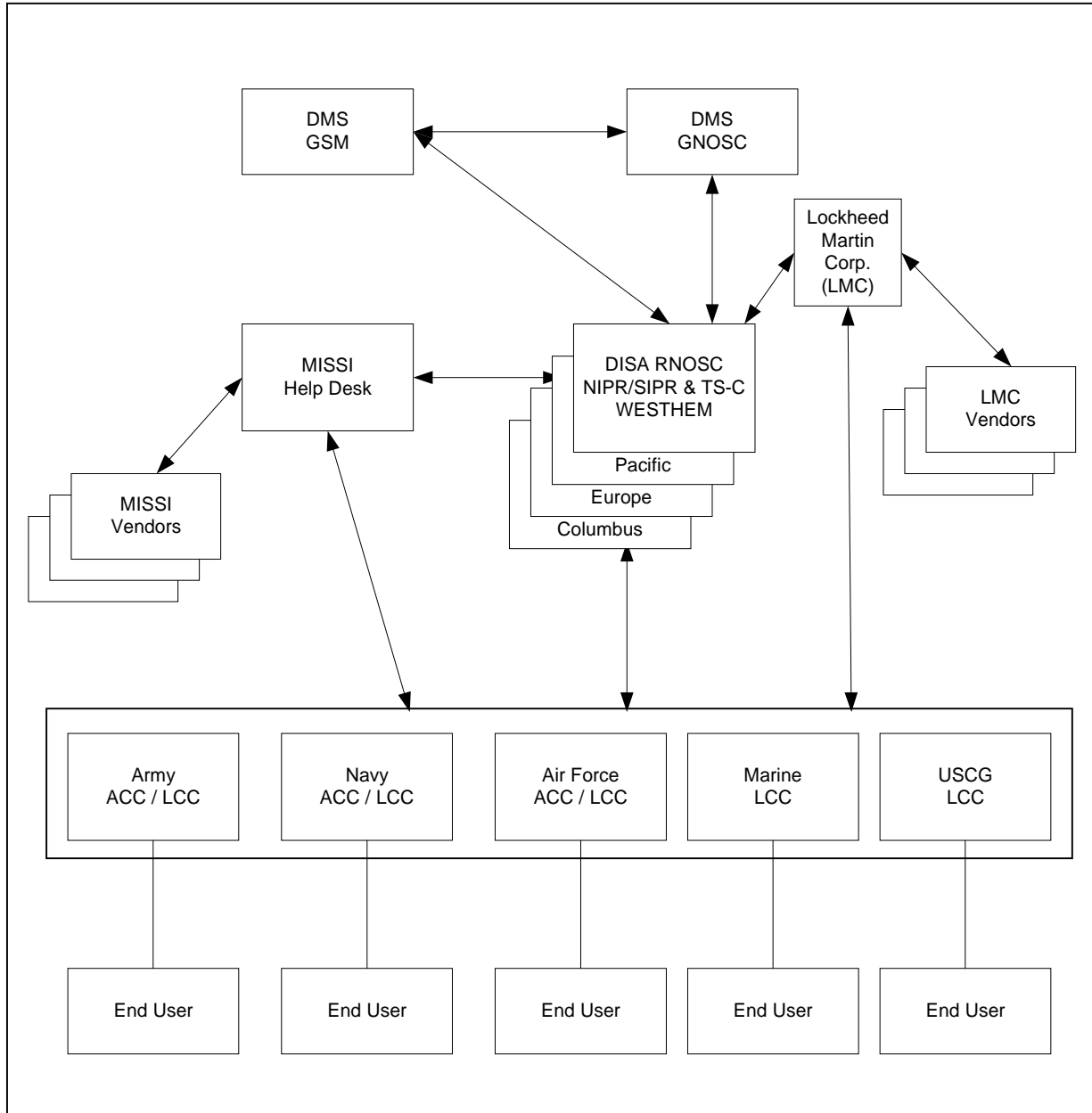


Figure 3-1

DMS Management Structure

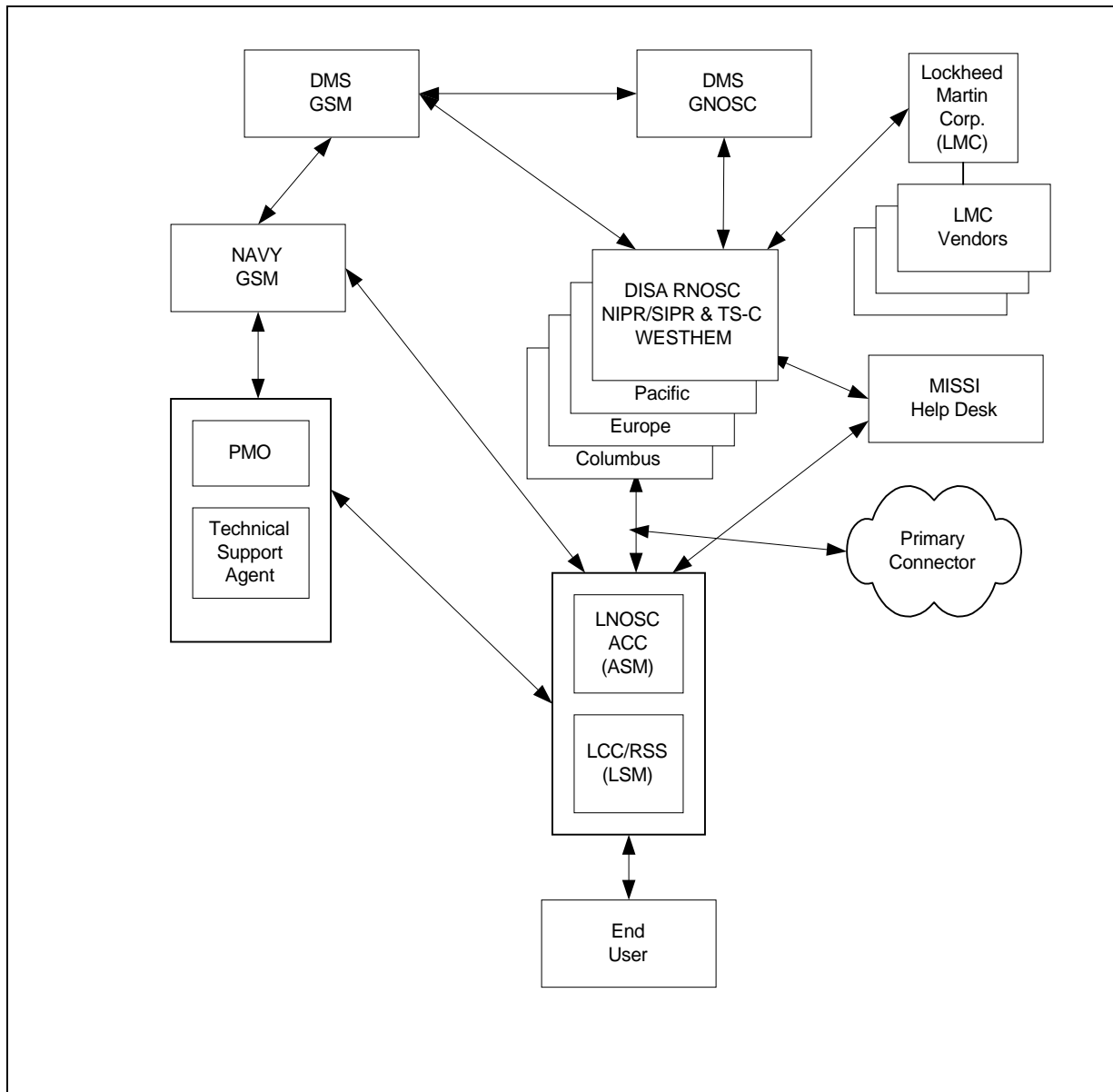


Figure 3-2

Navy Management Structure

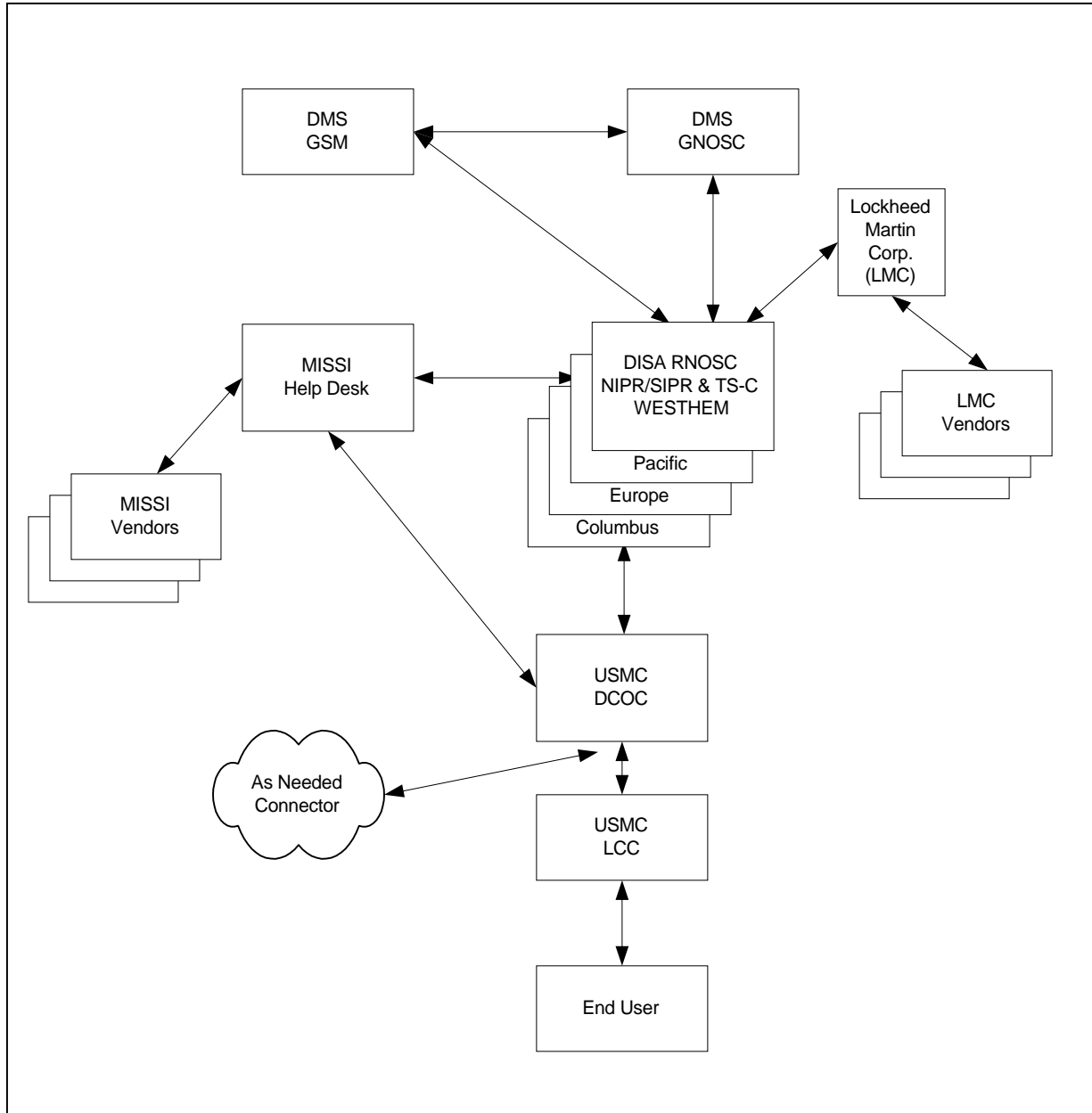


Figure 3-3

USMC Management Structure

**303. Regional Network Operations and Security Center (RNOSC)**

a. The DISA RNOSC supports the Regional System Manager (RSM) and performs proactive management of its area of the DMS. It does this by responding to conditions reported by the management protocol, the regional help desk, and by reports and trouble tickets elevated by the Navy LNOSC or other Service and Agency ACC'S or LCC'S. Depending on the condition involved, the response required may be simple or complex. RNOSC responsibilities are defined as all the regional node operations, transition hubs, and Service and Agency control centers within its geographic Area of Responsibility (AOR) or as identified by the GSM.

b. Each RNOSC is responsible for the operation and management of the DMS backbone, including regional nodes and DTH'S within its AOR. In addition, each RNOSC is responsible for providing service management support to the Navy LNOSC'S and USMC LCC'S located in its AOR. General responsibilities of the RNOSC are:

(1) Monitoring the DMS within its region and managing DMS messages to ensure that system efficiency is maintained.

(2) Maintaining the regional help desk to assist in resolving ACC, LCC, and User problems.

(3) Performing tracer actions on messages that transited the MTS segment within the RNOSC AOR.

(4) Analyzing problems elevated from the ACC'S or LCC'S, at the RNOSC or through referral to the appropriate analyst or technician.

c. There are four RNOSC'S, with locations and AOR'S as shown in Table 3-1, which also shows the unclassified operations message accounts assigned to each RNOSC for communications and coordination purposes. The RNOSC provides day-to-day, near real-time management of DISA assets throughout their respective regions. The AOR of the RNOSC-TS/C at Ft. Detrick, MD has been defined by the GSM as extending to the entire Top Secret Collateral portion of the DMS.

<b>RNOSC DESIGNATION</b>	<b>RNOSC LOCATION</b>	<b>Area of Responsibility</b>
RNOSC-Columbus (RNOSC-C)	Columbus, Ohio	Continental US, Canada, South and Central America, the Caribbean
US/U.S.Government/DoD/DISA/Organizations/GNOSC/RNOSC-Columbus/Controller		
RNOSC-Europe (RNOSC-E)	Stuttgart-Vaihingen, Germany	Continental Europe, United Kingdom, Middle East, Africa
US/U.S.Government/DoD/DISA/Organizations/GNOSC/RNOSC-Europe/ITACO1		
RNOSC-Pacific (RNOSC-P)	Pearl Harbor, Honolulu, Hawaii	Hawaii, Alaska, Far East, including Japan, the Philippines, Australia, New Zealand
US/U.S.Government/DISA/Organizations/GNOSC/RNOSC-Pacific/RNOSC-P2		
RNOSC-TS/C	Ft. Detrick, Maryland	Global Top Secret Collateral System
US/U.S.Government/DoD/AUTODIN PLAS/DTH Services/CONUS DTH(T)/DTH Operations Director(T)		

**Table 3-1****RNOSC Designations and Areas of Responsibility****304. Navy Local Network Operations and Security Center (Navy LNOSC)**

The Navy LNOSC may consist of an ACC, an LCC, or an RSS. In whatever role, Navy LNOSC'S provide network and messaging support to users at the local level and are the primary support for most DMS connectivity problems.

**304.1 Area Control Center**

The Navy DMS ACC operates, manages, and monitors a large geographical segment of the Navy's portion of the DMS. The ACC manages the subordinate LCC'S and RSS'S within its region and provides interface with the DISA RNOSC'S to resolve communications difficulties within their mutual areas of responsibility. In addition to managing Navy DMS resources within its area, the ACC also provides messaging services to DoN DMS Users. The ACC makes decisions for its entire region, rather than for a local area. There are four Navy ACC'S, located at NCTAMS LANT Norfolk, VA; NCTAMS EURCENT Naples, Italy; NCTAMS PAC Honolulu, HI; and NAVCOMTELSTA San Diego, CA.

### 304.2 Local Control Center

The Navy DMS LCC operates, manages, and monitors a medium size geographical segment of the Navy's portion of the DMS. The LCC provides functions and services that may not be available at an RSS.

### 304.3 Remote Service Center

The Navy DMS RSS operates, manages, and monitors a small geographical segment of the Navy's portion of the DMS. The RSS may operate a Help Desk and a Mail List Management function. Some RSS sites may not provide specialty component support; in those cases, that support will be provided by the LCC.

### 305. General Navy LNOSC Responsibilities

General Navy LNOSC responsibilities include:

- a. Providing Configuration Management within its region, site, or subordinate sites.
- b. Responding to fault conditions reported by the management protocol in the MWS.
- c. Initiating, monitoring, and closing trouble tickets. The ACC will escalate trouble tickets to the RNOSC as required.
- d. Monitoring traffic loads in the area of responsibility.
- e. Submitting periodic reports as outlined in CHAPTER 12.
- f. At the ACC, coordinating with the RNOSC for any interface problems between DISA DTH sites and DMS.
- g. Providing Help Desk assistance to DMS users for whom the Navy LNOSC provides support.
- h. Providing User Fortezza cards in support of organizational messaging.
- i. Providing MLA support for user Mail Lists.
- j. Providing X.500 Directory management in support of organizational messaging directory requirements.

A diagrammatic description of the Navy LNOSC'S, their locations, and their management and reporting relationships are found in CHAPTER 8.

**CHAPTER 4****OPERATIONAL ROLES AND RESPONSIBILITIES****401. General**

This chapter describes the roles involved in DoN DMS operations and the responsibilities of the DoN operation and management personnel to maintain the health and welfare of the DoN DMS infrastructure. These roles are defined as operations accounts necessary for communications between the RNOSC and Navy LNOSC sites and also with operational users. Each of the Managers has a DMS operations account as listed below.

**402. Defense Information Systems Agency (DISA)**

The DISA Deputy Director of Operations exercises executive management oversight of all DISA networks and facilities. This high-level management consists of establishing operational policies and procedures as well as providing system control over the DMS.

**402.1 DISA DMS Global System Manager (GSM)**

The DISA DMS GSM provides global management control and operational direction over the messaging services of the DII. As such, the GSM ensures customer requirements are satisfied in the most efficient, effective, economical, and responsive manner while maintaining system integrity, reliability, availability, and security to established management performance criteria. Not normally involved in day-to-day operations management, the DMS GSM is responsible for long-range planning, improvement of network efficiency, system enhancement, and planning and implementing new network interfaces and new services. The GSM is also the RSM for the Western Hemisphere region and has RSM responsibilities for that area. Note that as used here, the term "manager" applies to a function, usually a staff element, not to an individual person. Note that in this document, the term "GSM" always refers to the DISA DMS GSM. The Navy Global System Manager is referred to as the "Navy GSM".

**402.2 DISA DMS Regional System Manager (RSM)**

The DISA RSM performs many of the duties performed by the GSM at the global level. The RSM is the staff element associated with each RNOSC (WESTHEM, Europe, and Pacific). The RSM is responsible for providing guidance and real-time management direction to the RNOSC.

### 403. Navy Management Roles

#### 403.1 Commander Naval Computer and Telecommunications Command (COMNAVCOMTELCOM)

COMNAVCOMTELCOM, Washington D.C., is responsible for operating and maintaining the DoN segment of DMS. COMNAVCOMTELCOM provides systems and security management, develops policies and procedures, exercises control oversight for management of DoN ACC'S, LCC'S and RSS'S, and acts as service manager for all DoN customers. COMNAVCOMTELCOM is also the DMS Registration Authority (RA) for DoN. As such, COMNAVCOMTELCOM sets registration policy for the DoN and appoints Sub-Registration Authorities (SRA).

#### 403.2 Navy Global System Manager (Navy GSM)

The holder of the Navy GSM account provides global management and control of the DoN segment of the DMS and of Navy DMS assets. While not normally involved in day-to-day operations, the Navy GSM controls and directs the Navy LNOSC'S in operational matters, especially in the planning of authorized service interruptions, the application of software patches, and the implementation of system upgrades. The Navy GSM continuously monitors messages addressed to the Navy GSM account and takes action as required.

#### 403.3 Navy Area or Local System Manager (ASM or LSM)

Holders of Navy ASM and LSM accounts have responsibility for system management within the Navy LNOSC area of responsibility. Like the GSM and the RSM, the ASM and LSM have an operations account in order to coordinate and communicate vital network information to other accounts. It is DoN policy that only the ASM will communicate directly with the RNOSC; LSM'S will communicate with their designated ASM'S. The ASM and LSM are responsible for preparing a SOP for the Navy LNOSC as well as for users within their local area of responsibility. These SOP'S must conform to DISA and COMNAVCOMTELCOM policies. Local SOP'S are necessary because the wide variety of user component types and local conditions preclude the preparation of a general guidance document suitable for all localities. The ASM and LSM also are responsible for:

- a. Monitoring the ASM and LSM operations accounts and taking action as required.
- b. Preparing local routing plans for each Navy LNOSC PGWS, with changes needed to deal with component failure.
- c. Supervising operation of the Help Desk, advising and assisting in preparation of trouble tickets, and directing elevation of trouble tickets to the RNOSC as necessary (see CHAPTER 8).



- d. Evaluating and coordinating DIB distribution among DSA'S, including shadowing agreements.
- e. Evaluating current component operations to determine if additional DMS components are needed, or if current components are no longer needed.
- f. Establishing service priorities for users.
- g. Performing message traces as required (see CHAPTER 9).
- h. Ensuring that required reports are prepared and submitted as required (see CHAPTER 12).
- i. Establishing Navy LNOSC component backup criteria and ensuring that backups are performed (see CHAPTER 17).
- j. Developing and maintaining a local Configuration Database and passing it to the DISA RSM for inclusion in the regional Configuration Management (CM) database.
- k. Collecting audit records from the local DMS components, reviewing, and retaining Navy LNOSC security audit trail data as directed by the Designated Approving Authority (DAA).
- l. Coordinating with the ISSO on any security problems within the Navy LNOSC or in components within the Navy LNOSC area of responsibility.
- m. Distributing new software releases.
- n. Carrying out DMS policies and procedures and reporting violations to the command authority.
- o. Maintaining an inventory of accountable assets.
- p. Coordinating with the RNOSC and the RSM for routing of message traffic for users transitioning to DMS.

#### **404. Navy Mandatory Roles**

##### **404.1 DoN Sub-Registration Authority (SRA)**

COMNAVCOMTELCOM, as DoN Primary RA, appoints SRA accounts to manage the distinguished name process for the DoN. The SRA is delegated authority over lower areas of the Directory. The upper level (parent) SRA must be aware of the identity of the lower level (child) SRA'S. SRA'S are responsible for actually making and modifying Directory entries for users in their assigned areas. SRA'S may delegate user interface functions to an Organizational Registration Authority (ORA) or may exercise ORA responsibilities. If the SRA exercises ORA functions, duties of the SRA will also include those listed below for the ORA. Duties specific to the SRA are:

- a. Registering the Organizational Unit (OU) field below the O=[Service/agency name], and registering infrastructure component names.
- b. Registering Directory Distinguished Name (DDN) requests from the ORA and ensuring global uniqueness of a user's DDN.
- c. Maintaining records of DDN'S within the SRA'S AOR.
- d. Accepting user registration requests and approving or rejecting them within two working days.
- e. Receiving DDN requests from the ORA and creating the Directory entry, including operational and user information.
- f. Posting the authorized information into the Directory.
- g. Registering O/R addresses.

The SRA is responsible for the final step in establishing an organization account, which is to establish a PLA to X.500 Distinguished Name (DN) association. This process requires actions by the ORA, LNOSC SRA, and the DISA PLA Directory Administrator. The procedures for establishing a PLA - X.500 association are detailed below. These procedural steps must be executed in the order shown.

(1) The organization's ORA must coordinate with the assigned SRA to verify directory information and accomplish certain local directory changes. When the organization's directory information has been updated, validated, and deemed ready for DMS activation, the SRA must update the Point of Contact (POC) organizational unit entry to include the PLA DN in the associated PLA field. The steps to follow in implementing these changes are shown below.

- (a) Zoom out to level 3 (DoD). Once at level 3, browse down to the POC organizational unit whose associated PLA attribute is to be populated.
- (b) Open the properties of the POC organizational unit (right click) and then click on the reference tab.
- (c) Click modify.
- (d) Click change on associated PLA.
- (e) Directory will open up to DoD. Browse down to the GENSER PLA sub-tree.
- (f) Open the tree to the appropriate PLA.

NOTE: This will work only if the PLA is an existing PLA. If a new PLA is being created for the organization and has not yet been added to the PLA DSA, the SRA must type the PLA DN in the *associatedPLA* attribute field.

- (g) Double click the PLA entry.
- (h) The associated PLA field is now populated.
- (i) Select apply and OK.

(2) The SRA will then provide the PLA Directory Administrator, located at Ft. Detrick, MD, with the PLA and associated organization DN information.

NOTE: This information must be contained in an ASCII text file created in the exact format specified below.

EXAMPLE:

```
PlaName: PM DMS-ARMY FT MONMOUTH NJ  
AssociatedOrganization: ou=PROJECT MANAGER(n),ou=PM  
DMS-ARMY,l=FORT MONMOUTH NJ,l=CONUS,ou=Organizations,  
ou=Army,ou=DoD,o=U.S. Government,c=US
```

NOTE: The SRA must send this ASCII text file as an attachment to a DMS encrypted, signed message so that the PLA Directory Administrator (DA) can authenticate that the message is from an authorized SRA. The file should be sent to the following X.500 address:

```
c=US/o=U.S. Government/ou=DoD/ou=AUTODIN PLAs/ou=DTH  
Services/ou=CONUS DTH/ou=DTH Operations Director
```

(3) If the organization plans to use office codes to allow messages to be addressed and delivered directly to the sub-organizations, the SRA must inform the PLA DA to enter the value "YES" in the *plaRemarks* attribute of the GENSER PLA entry associated with the sub-organization's parent entry. This request to the PLA DA must be sent to the same X.500 address shown above.

(4) The PLA Directory Administrator will notify the SRA once the changes have been completed.

(5) The SRA should prepare the appropriate request to update the PLA information in the Message Conversion System Central Directory Component (MCS CDC), which provides PLA-to-Routing Indicator (RI) conversion in the legacy systems. This update will include the addition of the MFI RI to the list of RI'S associated with the PLA. The SRA should send this request to his or her respective Service or Agency Military Communications Procedures Permanent Working Group (MCP PWG) member.

- (6) The information required must include the following:
- (a) Effective date of proposed change.
  - (b) Action to be taken: ADD, CHANGE, or DELETE.
  - (c) Routing information (in columnar format).

EXAMPLE:

**Effective 1 December 2000.**  
**Action Required: Change**  
**Columnar Data.**

COL A: PM DMS ARMY FT MONMOUTH NJ  
 COL B: RUERMOO  
 COL C: B  
           RHMFIUU  
 COL D: B  
 COL E : S  
           A

NOTE: If dual routing is being requested, the specific time frame that dual routing will be used should be specified.

The effective date should allow sufficient time for the organizational unit entry and the GENSER PLA entry to be mapped to each other. If the mapping has already taken place, the effective date can be set to "Immediate".

(7) Action(s) are now complete and the DMS user's UA Terminal can now receive messages originated in the DTH legacy system.

#### **404.2 Organizational Registration Authority (ORA)**

The ORA is a mandatory role at the Navy organizational level. The ORA is appointed by the Commander of an organization with the approval of the SRA. An ORA, if appointed, acts as the intermediary between the CA, the SRA, and the user. As a member of the user's organization, the ORA verifies the identity of prospective users in the organization and takes appropriate action to register them and obtain Fortezza cards. The ORA will normally pass Fortezza cards obtained by the CA to the user. ORA'S should be persons of proven honesty and integrity. ORA'S should know personally each prospective user or at least know each supervisor. The duties of an ORA include:

- a. Verifying the identity of prospective users and ensuring that they are properly sponsored.
- b. Verifying the uniqueness of the user's Directory Distinguished Name and assigning one if necessary.

- c. Verifying the accuracy of the information in the certificate request.
- d. Completing the X.509 certificate request and signing the request before submitting it to the CA.
- e. Gathering user information and coordinating with the SRA for the registration of the user's DDN.
- f. Forwarding requests for Fortezza cards to the CA.
- g. Ensuring that the security clearance and access level of prospective users (including organizational release authorities) have been verified by the Organizational Security Officer (OSO) and that the access level is appropriate to the user's security clearance.
- h. Receiving programmed Fortezza cards from the CA and distributing them to the appropriate users, obtaining the user's handwritten signature, and returning it to the CA.
- i. Ensuring proper control and inventory of any Fortezza cards in the ORA'S possession.
- j. Notifying the CA and OSO of Fortezza card loss, theft, damage, or destruction.
- k. Initiating the de-registration process for users leaving the organization or base and returning Fortezza cards to the CA for reprogramming.

#### **404.3 Organizational System Administrator (OSA)**

The OSA account holder is responsible for all the DoN DMS components within the OSA AOR, and the responsibilities listed below apply to all components. While most DMS components are designed to operate continuously in an unattended mode, some administrative functions are required on a periodic basis. The principal one of these functions is the system backup. A backup in this case means the transfer of log and audit data from the system internal storage (hard disk) to an external storage device (CD-ROM or tape) for the required retention period. CHAPTER 17 describes backups and their required frequency. Other duties of the Systems Administrator include:

- a. Monitoring the SA operations account and taking action as required.
- b. Preparing an SOP for the administration and use of the various components within the AOR.
- c. Analyzing problems or assisting local or regional DMS Analysts in doing so.

d. Overseeing or performing the installation of new hardware and software and monitoring hardware upgrades.

e. Configuring software, including installing new software releases, applying patches, verifying checksums to ensure software validity, and notifying the ASM or LSM and the Navy LNOSC Help Desk of the installation of a new release (see CHAPTER 10 and CHAPTER 11).

f. Ensuring that software installed on a new or upgraded component is the latest version and includes the latest changes.

g. Coordinating hardware repairs, preventive maintenance, and upgrades with the Maintenance Technician.

h. Conducting liaison with the serving Navy LNOSC Help Desk (HD) when user interface is required. Only the organizational SA is authorized to initiate contact with the Navy LNOSC.

i. Conducting audit trail review in support of trace requests when automated tools are not available.

j. Coordinating with management personnel to detect and report software deficiencies, operating deficiencies, or documentation deficiencies in the AOR.

k. Performing the initial system configuration including boot start up and shut down processes, initializing and re-initializing components as necessary, and performing hands-on management functions that cannot be done from the MWS.

l. Coordinating with the appropriate Security Officer to investigate and resolve security problems.

m. Performing archive and delete functions of the audit log as recommended by the OSO.

n. Analyzing claims of non-delivery and submitting Message Trace Requests to the Navy LNOSC Help Desk as required.

o. Performing reconfiguration of components.

p. Initiating the registration process for the infrastructure components with the SRA.

q. Establishing a process for registering each component with adjacent components to allow proper authentication and for distributing the means of authentication (such as passwords).

r. Requesting Fortezza cards for components when strong authentication is implemented.

s. Assisting the OSO as required by the Information System Security Program.

#### 404.4 Organizational Security Officer (OSO)

The OSO is a mandatory role and operations account holder. The OSO is responsible for enforcement of security policies and doctrines for the portion of the DMS within the OSO'S Area of Responsibility. The OSO is responsible, at the local level, for enforcement of security policies and doctrines. Part of this role is the auditing of users and managers for compliance with security procedures. This includes oversight of SRA'S, ORA'S, and CA'S to ensure that users are assigned proper access attributes, analysis of security-related events, and analysis of security violations or failures with recommendations for changes to prevent recurrence. To ensure the integrity of X.509 certificates, an OSO may not perform CA functions or have access to the CA Fortezza cards. OSO'S are appointed by the head of the organization and must be persons of proven trustworthiness and integrity. In general, OSO'S are responsible for:

- a. Monitoring the OSO operations account.
- b. Reviewing all CIAC/NAVCIRTS, IAVAs and related vulnerability attack notices.
- c. Enforcing DMS network security and risk management policies.
- d. Developing an accreditation plan.
- e. Establishing and maintaining internal policies and procedures that provide for the physical security of DMS facilities and the integrity and security of DMS components.
- f. Coordinating with the command Security Manager to provide the appropriate physical security and access restrictions for DMS components and platforms.
- g. Preparing and maintaining contingency plans for the preservation of security in the event of a natural disaster, enemy or terrorist attack, or the threat of such an attack.
- h. Performing security audits of those DMS components within the OSO'S AOR.
- i. Reviewing, on a daily basis, security event audit reports by component.
- j. Ensuring compliance with system level security audit requirements.
- k. Overseeing security policies and practices for DMS components.

l. Participating, as necessary, in the review and analysis of any security violations.

m. Coordinating with the SA in the recognition of security threats and weaknesses in DMS components and reviewing problems having security implications, such as message non-delivery, denial of service, or unauthorized system penetration.

n. Ensuring the implementation and maintenance of access control policy and procedures to protect the DMS components and services from unauthorized access, use, and manipulation.

o. Ensuring that the SRA'S, ORA'S, and CA'S at the installation follow access guidelines, provide proper security access validation, and prepare Fortezza cards and certificates with the correct security attributes.

p. Ensuring that appropriate mechanisms (software, hardware, procedural, or administrative) are in place to monitor security threats to, and vulnerabilities of DMS components and services.

q. Ensuring that ORA'S, CA'S, and users exercise proper control of Fortezza cards and assist ORA'S and CA'S in inventory control of these cards.

r. Investigating any loss or accidental destruction of a Fortezza card and determining if any security compromise has occurred.

s. Preventing delay in implementing required changes when security information becomes compromised or obsolete (e.g., an authorized user leaves the installation or loses a Fortezza card).

t. Monitoring and implementing management and reporting procedures for DMS security incidents and technical vulnerabilities.

u. Investigating security violations within the OSO'S AOR.

#### **404.5 Certification Authority (CA)**

The CA role is established at the LNOSC, large installations, and major claimant sites to support the creation, issuance, and management of Fortezza cards. The CA creates DMS Organizational User messaging identities and security credentials that are encoded into Fortezza cards. The CA works under the control of three DMS security entities: the Policy Approving Authority (PAA), the Policy Creation Authority (PCA), and the Certificate Approving Authority (CAA). DoN CA'S are normally appointed by the DoN CAA to serve at LNOSC sites and support users within a geographical area. However, local commanders and approving authorities at major claimant sites may request the DoN CAA to



appoint local CA'S to meet DoN DMS implementation objectives. The principal functions of the CA'S are:

- a. Creating, updating, and accounting for cryptographic and signature keys. (See Note.)
- b. Ordering, programming, and distributing Fortezza cards.
- c. Adding, managing, and deleting DMS directory certificate information using information obtained from the ORA.
- d. Interacting directly with users, as well as through the ORA.
- e. Revoking certificates and Fortezza cards as necessary, creating and distributing the Certification Revocation List (CRL), coordinating with the security root CA when necessary.
- f. Providing for continued operation during certificate expiration by, for example, preparing new cards in advance of need for users whose certificates are about to expire.
- g. Maintaining X.509 form files as required.
- h. Passing to the security root reports of any local incidents that will require an addition to the Compromise Key List (CKL).

Note: CA'S must be aware that certificates and Fortezza cards must explicitly identify each security classification that the user is authorized to select. Unlike older access control mechanisms, access to a high level (e.g., Secret) does not automatically grant access to lower classifications (e.g., Confidential). Each security classification authorized to the user must be set separately.

#### **404.6 Mail List Manager (MLM)**

The MLM is responsible for the maintenance of every DoN Mail List within an AOR. DoN MLM'S are designated by NAVCOMTELCOM. The MLM deals specifically with the creation, modification, and removal of Mail Lists from the Directory through the use of an ADUA. During Mail List maintenance, the MLM interfaces with the cognizant authority, the CA, and the PLA Administrator in the legacy system. Additionally, the MLM deals with the details of installation and removal of Fortezza Cards as well as any MLA configuration changes necessary to activate or deactivate a Mail List. The MLM will assist the cognizant authority in the process of transitioning legacy collective users and members to DMS Mail Lists. The MLM is also responsible for the configuration of MLA'S. The duties of the MLM include:

- a. Creating and updating the Mail List in the X.500 Directory, using the associated Mail List certificates and some

initial attributes provided by the local CA and ORA'S; nesting Mail Lists as necessary to provide optimum processing.

b. In coordination with the CA and ORA, determining which users should have submission privileges to the Mail List and provide permission for usage.

c. Determining Mail List placement on a MLA by evaluating the purpose, criteria, membership, and frequency of use of the Mail List, and setting up a storage area on the MLA for on-line storage of audit trail data.

d. Coordinating with the CA to program the Mail List identity onto a Fortezza card and post the certificate to the directory and ensuring the Routing Configuration Data Base (RCDB) and MLA configuration information are updated to service the Mail List.

e. Invalidating the current MLA cache and downloading the revised Mail List from the X.500 Directory to the MLA cache whenever changes are made.

f. Following up non-delivery reports to resolve possible addressing errors and identify expired certificates or outdated addresses.

g. Establishing limits on the classification of submitted messages in accordance with direction from the cognizant authority.

#### **404.7 Navy LNOSC Help Desk (HD) Specialist**

The Navy HD specialist account holder acts as the customer point of contact at the Navy LNOSC. The duties involved with this account are assisting customers, resolving complaints on first contact if possible, and coordinating with the ASM or LSM in opening and closing trouble tickets when appropriate. The HD specialist will elevate tickets to the RNOSC only with the approval of the LSM. The HD specialist also reviews open trouble tickets and monitors their status.

While it is the duty of the HD specialist to answer general questions from current and prospective DMS users, if a question or its answer would appear to violate security guidelines, HD personnel will refer the caller to the LSM. Examples would include such questions as the number of users, their locations, exact location of the Navy LNOSC, message security procedures, and message statistics. Other duties include:

a. Monitoring the HD organizational message account and taking action as required.

b. Answering questions posed by users or potential users of the DMS about its operations and its services.

c. Assisting users in resolving DMS related problems and determining when a user question or concern requires writing a trouble ticket.

d. Writing trouble tickets in sufficient detail to allow accurate diagnosis and prompt resolution of the problem, passing trouble tickets to the LSM for escalation as required, and requesting technical support as necessary.

e. Maintaining a historical database of all reported problems, their resolutions, and associated events and observing and reporting trends. Providing users with periodic status reports on open trouble tickets.

f. Reviewing daily all open trouble tickets and providing the ASM or LSM a daily status report of open trouble tickets.

g. Providing general DMS information to the users on new software, Directory use, bulletins, planned service interruptions, and other information that may impact the user's messaging.

h. Notifying the DMS security officer of any actual or attempted violations of DMS security policies or procedures.

i. Maintaining a historical database of all reported problems, the actions taken for resolution, and any associated relevant events.

j. Coordinating with the user to ensure a satisfactory resolution before closing a trouble ticket that was opened at a user's request.

k. Developing and publishing DMS customer service survey statistics.

l. Assisting with the preparation and submission of the required daily and monthly DMS reports.

m. Reviewing non-delivery claims and submitting message trace requests from the user's OSA to the ASM or LSM for further action.

n. Reviewing the trouble ticket historical file for identification of recurring or systemic problems and their previous resolution.

#### **404.8 Navy Area or Local System Manager (ASM or LSM)**

Holders of Navy ASM or LSM accounts have responsibility for system management within the Navy LNOSC area of responsibility. Like the GSM and the RSM, the ASM or LSM has an operations account in order to coordinate and communicate vital network

information to other accounts. It is DoN policy that only the ASM will communicate directly with the RNOSC; LSM'S will communicate with their designated ASM'S.

#### **404.9 Operations Manager (OM)**

The OM role is appointed by the LSM to perform as the day-to-day supervisor of the LNOSC operation. The OM is responsible for ensuring that LNOSC personnel perform their assigned duties and that required operations are carried out. The LSM or ASM may delegate responsibilities and authority to the OM as necessary as contained in the LNOSC SOP and may authorize the OM to use the ASM or LSM account during other than normal business hours.

#### **405. U.S. Marine Corps Management Roles**

a. The USMC DCOC, as part of the MITNOC, is responsible for operating and maintaining the USMC segment of DMS. The DCOC provides system and security management, configuration management, Mail List management, Directory management, and central Help Desk. Additionally, the DCOC will act as the DMS Registration Authority for the USMC.

b. The DCOC, as the USMC Registration Authority, delegates Directory management functions to site SRA'S. It is not the intent of the USMC to formally delegate registration management down to the organizational level. Organizations will submit required changes to the supporting ACC or LCC SRA where modifications to the directory will be accomplished. The DCOC will develop Standard Operating Procedures for directory change or modification. SRA'S will develop local operating procedures that will encompass all registration issues.

c. Duties specific to the SRA are commensurate with those outlined in Paragraph 404.1 and 404.2.

d. The CA roles and responsibilities as outlined in Paragraph 404.5 apply to the USMC. The physical location of the CA may be either within the LCC or at one or more of the major subordinate commands, as determined by the installation commander.

e. Centralized Mail List Management and Help Desk service are roles of the DCOC. These roles and responsibilities as outlined in Paragraphs 404.6 and 404.7 apply to USMC sites. Sites will establish a Help Desk capability to support local issues and problems. During the initial transition, Mail Lists will be maintained at the site where the cognizant authority resides. In the future, all USMC Mail Lists will be maintained at the DCOC.

CHAPTER 5DON DMS OPERATIONAL ROLES AND ACCOUNTS**501. General**

This chapter describes the necessary roles and associated active accounts necessary to maintain the health and welfare of the DoN DMS infrastructure. These accounts provide the necessary communications between the RNOSC, the Navy LNOSC, and the users to provide critical DMS services.

**502. Operations Accounts**

DoN requires that each Navy and USMC system manager and authority have an operations message account to exchange vital DMS information with other managers and with the RSM. Once an account is established, the holder of the account will forward a signed and encrypted organizational message to the next higher account, identifying the X.500 DN of the designated DMS Operations Account. The message will be released from the designated account. Normally, this is accomplished as part of the site acceptance and commissioning process, but if it is not already established or if the account is changed, the site shall identify it to the RNOSC as stated above. The RNOSC in turn will identify the subordinate Navy LNOSC Operations Accounts to the GSM.

a. The following accounts will be established for DoN:

- (1) Commander, Naval Computer and Telecommunications Command (COMNAVCOMTELCOM).
- (2) DoN Global System Manager (GSM).
- (3) USMC DMS Control Operations Center (DCOC).

b. The following accounts have been established for Navy LNOSC'S and Navy Organizations:

- (1) Navy Area System Manager (ASM).
- (2) Navy Local System Manager (LSM).
- (3) Navy Help Desk (HD) Specialist.
- (4) Navy Sub-Registration Authority (SRA).
- (5) Navy Organizational Registration Authority (ORA).
- (6) Navy Organizational System Administrator (OSA).
- (7) Navy Organizational Security Officer (OSO).
- (8) Navy Mail List Manager (MLM).

c. USMC specific positions will be added to the Directory as the DCOC becomes functional.

### 503. Registration Criteria for Navy Role Names

This section presents the naming conventions for the assignment of Relative Distinguished Names (RDN) for the Navy's LNOSC'S, the roles supporting these Control Centers, the Certification Authorities, and the Navy Registration Authorities. It also includes the naming conventions for three roles to be supported by every Navy organization that uses the DMS. These roles include the ORA, the OSA, and the OSO.

#### 503.1 Symbols and Capitalization Rules

a. Listed below are the special naming constructs used in describing the format for the various conventions defined in this section.

- (1)  $\Delta$  represents a "space" character.
- (2) *planame* represents a PLA with location information.
- (3) *level-7* represents Level-7 entries RDN value (city, base, post, camp, station). For ships and mobile units, use entire *planame*.
- (4) *level-6* represents the Level-6 entries RDN value mapped to two characters (Virginia=VA, Italy=IT). If level-7 represents the RDN of a ship or mobile organization, level-6 is not used.
- (5) *nnnn* is a sequence number.
- (6) *S* represents the sensitivity.
- (7) *rolename* is a standard role name.
- (8) - is the actual dash character.

b. Listed below are the capitalization rules for the naming constructs to be applied when creating the RDN values for Control Centers and roles.

- (1) *planames* ALL CAPITALS.  
Ex: NCTAMS LANT NORFOLK VA
- (2) *level-7* Mixed Case is required.  
Ex: Norfolk
- (3) *level-6* Mixed Case is required.  
Ex: Va
- (4) *S* CAPITAL.  
Ex: U
- (5) *rolename* ALL CAPITALS.

Ex: ORGREGAUTH and SECURITY-OFFICER

### 503.2 Standard Role Names

Table 5-1 contains a list of the standard role names currently defined for DMS management at the LNOSC'S and the mandatory roles at the DMS organization. The paragraphs following the table provide additional details about each of the role names.

LNOSC Role Name*	LNOSC Role Function	Level
ASM ... (M)	Area System Manager	10
CERTAUTHnnnn... (M)	Certification Authority (uses sequence numbers to further distinguish this role)	5
CONFIGMNGR... (M)	Configuration Manager	10
DIRADMINnnnn... (O)	Directory Administrator (uses sequence numbers to further distinguish this role)	10
DMSOPSMNGR-... (M)	DMS Operations Manager	6
GSM NAVY-... (M)	General System Manager for the Navy	6
HELPDESK... (M)	Helpdesk	10
LSM ... (M)	Local System Manager	10
MLADMINnnnn... (O)	Mail List Administrator (uses sequence numbers to further distinguish this role)	10
MLMANAGER... (M)	Mail List Manager	10
REGAUTH NAVY-... (M)	Registration Authority for the Navy	6
REGAUTH PRIMARY-. (M)	Primary Registration Authority for Navy	6
REGAUTH SECONDARY-(M)	Secondary Registration Authority for Navy	6
SECURITY-OFFICER.. (M)	Security Officer	10
SUBREGAUTH... (M)	Sub-Registration Authority	10
MANDATORY ROLES (Mandatory)		
ORGREGAUTH... (M)	Organizational Registration Authority	8 or 9
ORGSECOFF... (M)	Organizational Security Officer	8 or 9
ORGSYSADMIN... (M)	Organizational Systems Administrator	8 or 9

\*Additional roles may be added to the table as needed.

**Table 5-1**

**Standard Management Role Names**

### 503.3 Certification Authorities

Certification Authorities are at level-5 of the Directory Information Tree (DIT) under OU=Navy.

Name format is CERTAUTHnnnn $\Delta$ (S-planame).

EXAMPLE:

C=US /O=U.S. Government / OU=DoD / OU=Navy /  
CN=CERTAUTH0001 (U-NCTAMS LANT NORFOLK VA)

### 503.4 Registration Authorities

Registration Authorities are at level-6 of the DIT under OU=Navy / OU=Organizations.

Name format is REGAUTH $\Delta$ NAVY-planame,  
REGAUTH $\Delta$ PRIMARY-planame,  
REGAUTH $\Delta$ SECONDARY-planame.

EXAMPLE:

CN=REGAUTH NAVY-COMNAVCOMTELCOM WASHINGTON DC(n)  
CN=REGAUTH PRIMARY-NAVCOMTELSTA WASHINGTON DC(n)  
CN=REGAUTH SECONDARY-NCTAMS LANT NORFOLK VA(n)

### 503.5 Navy Global System Manager

The Navy's Global Systems Manager is at level-6 of the DIT under OU=Navy / OU=Organizations.

Name format is GSM $\Delta$ NAVY-planame.

EXAMPLE:

CN=GSM NAVY-COMNAVCOMTELCOM WASHINGTON DC(n)

### 503.6 Navy DMS Operations Manager

The Navy's DMS Operations Manager is at level-6 of the DIT under OU=Navy / OU=Organizations.

Name format is DMSOPSMNGR $\Delta$ NAVY-planame.

EXAMPLE:

CN=DMSOPSMNGR NAVY-COMNAVCOMTELCOM WASHINGTON DC(n)

### 503.7 Area Control Center Names

Area Control Center names are at level-9 of the DIT under their corresponding organization's PLA entry. The ACC name is not a role name, but it is listed in this section because the ACC must be registered before the roles at the ACC can be registered.

Name format is ACC $\Delta$ level-7 $\Delta$ level-6.

EXAMPLE for the ACC at Norfolk Virginia:

OU=NCTAMS LANT NORFOLK VA (n) / OU=ACC Norfolk Va(n)



### 503.8 Local Control Center

Local Control Center names are at level-9 of the DIT under their corresponding organization's PLA entry. The LCC name is not a role name, but it is listed in this section because the LCC must be registered before the roles at the LCC can be registered.

Name format is `LCCΔlevel-7Δlevel-6`.

EXAMPLE for the LCC at Jacksonville Florida:

`OU=NAVCOMTELSTA JACKSONVILLE FL (n)/OU=LCC Jacksonville Fl(n)`

### 503.9 Remote Server Site

Remote Server Site names are at level-9 of the DIT under their corresponding organization's PLA entry. The RSS name is not a role name, but it is listed in this section because the RSS must be registered before the roles at the RSS can be registered.

Name format is `RSSΔlevel-7Δlevel-6`.

EXAMPLE for the RSS at Hampton Roads Norfolk Virginia:

`OU=NCTAMS LANT DET HAMPTON ROADS NORFOLK VA(n)/`

`OU=RSS Hampton Roads Norfolk Va(n)`

### 503.10 Mandatory Role Names for Management Centers

Mandatory role names for management centers are at level-10 under their corresponding level-9 LNOSC entries.

Name format is `rolenameΔlevel-7`.

EXAMPLE for ASM for the ACC at Norfolk:

`OU=NCTAMS LANT NORFOLK VA(n)/`

`OU=ACC Norfolk Va(n)/`

`CN=ASM Norfolk(n)`

EXAMPLE for LSM for the LCC at Jacksonville Fl:

`OU=NAVCOMTELSTA JACKSONVILLE FL(n)/`

`OU=LCC Jacksonville Fl(n)/`

`CN=LSM Jacksonville(n)`

EXAMPLE for Security Officer at the RSS Hampton Roads:

`OU=NCTAMS DET HAMPTON ROADS NORFOLK VA(n)/`

`OU=RSS Hampton Roads Norfolk Va(n)/`

`CN=SECURITY OFFICER Hampton Roads Norfolk(n)`

EXAMPLE for MLM at the LCC Jacksonville Fl:

`OU=NAVCOMTELSTA JACKSONVILLE FL(n)/`

`OU=LCC Jacksonville Fl(n)/`

`CN=MLMANAGER Jacksonville(n)`

EXAMPLE for SRA at LCC Jacksonville Fl:

`OU=NAVCOMTELSTA JACKSONVILLE FL(n)/`

`OU=LCC Jacksonville Fl(n)/`

`CN=SUBREGAUTH Jacksonville(n)`

EXAMPLE for Configuration Manager at LCC Jacksonville Fl:

```
OU=NAVCOMTELSTA JACKSONVILLE FL(n)/
OU=LCC Jacksonville Fl(n)/
CN=CONFIGMNGR Jacksonville(n)
```

EXAMPLE for Helpdesk at LCC Jacksonville Fl:

```
OU=NAVCOMTELSTA JACKSONVILLE FL(n)/
OU=LCC Jacksonville Fl(n)/
CN=HELPDESK Jacksonville(n)
```

### 503.11 Optional Role Names for Management Centers

Optional role names for management centers are at level-10 under their corresponding level-9 LNOSC entries.

Name format is *rolename*Δ*level-7*.

EXAMPLE for MLA at the LCC Jacksonville Fl:

```
OU=NAVCOMTELSTA JACKSONVILLE FL(n)/
OU=LCC Jacksonville Fl(n)/
CN=MLADMIN1 Jacksonville(n)
```

EXAMPLE for DA at the LCC Jacksonville Fl:

```
OU=NAVCOMTELSTA JACKSONVILLE FL(n)/
OU=LCC Jacksonville Fl(n)/
CN=DIRADMIN5 Jacksonville(n)
```

### 503.12 Mandatory Organizational Roles

There are three mandatory organizational roles for every organization registered in DMS. These roles are the ORA, the OSA, and the OSO.

Name format is *rolename-planame*.

EXAMPLE for each organizational role at Chief of Naval Operations (CNO) WASHINGTON DC:

```
CN=ORGREGAUTH-CNO WASHINGTON DC(n)
CN=ORGSYSADMIN-CNO WASHINGTON DC(n)
CN=ORGSECOFF-CNO WASHINGTON DC(n)
```

### 504. USMC Registration Criteria

USMC Registration Criteria are still being developed and will be promulgated separately and incorporated in this document at a later date.

**CHAPTER 6****NAVY LNOSC OPERATING PROCEDURES****601. General**

This chapter describes the operating procedures to be followed by Navy LNOSC personnel. The role responsible for direct supervision of LNOSC activity is the Operations Manager, working under the authority of the LSM.

**602. RADAY Change Procedures****602.1 Reports**

The following reports are required at change of RADAY or as soon as possible thereafter.

- a. System Status Report.
- b. Cumulative Statistics Report.
- c. Daily Navy LNOSC Summary Report.
- d. Daily Navy LNOSC System Performance Report.

**602.2 Audit Collection**

As soon as possible after RADAY change, the audit reports and audit trail data from the DMS components for the previous RADAY must be collected, reviewed, and retention ensured as required by DISA and COMNAVCOMTELCOM. This is the duty of the OSA and the OSO.

**602.3 System Backups**

The OSA must ensure that system backups are performed. System backups must be performed on a regular schedule, in accordance with the Navy LNOSC SOP. This is normally done near RADAY change, but it is not associated specifically with that time.

**602.4 Help Desk Logs**

The HD specialist must ensure that HD trouble reports and other required hard copy logs are closed out and filed.

**602.5 Operations Message Files**

Each operations role is responsible for filing all operations messages.

**603. Shift Change Procedures**

a. The Operations Managers will ensure that operation of the LNOSC is maintained under controlled conditions during shift changes. Shift turnover will occur anytime that one shift

relieves another and will occur at a time established by the LSM. Shift turnover procedures will ensure that:

(1) The transition is carried out with minimal customer impact.

(2) The transfer of pertinent information will take place.

(3) There will be an adequate discussion of events, procedures, and techniques between the departing and arriving Operations Managers.

b. Prior to shift change, the on-duty Operations Manager will ensure that:

(1) The master station log has been updated with all pertinent information.

(2) Outstanding trouble tickets have been reviewed and properly annotated.

(3) The work area is clean and uncluttered.

c. The Operations Manager reporting on-duty will:

(1) Review the station log.

(2) Review and assess trouble tickets for completeness and priority.

(3) Review inventories and take appropriate action in the event of discrepancies. This may include conducting a second inventory, retaining outgoing personnel, or conducting searches.

(4) Ensure the work area is clean and uncluttered.

d. During shift change, the outgoing and the incoming persons responsible for accountable material must conduct a joint inventory of such material and both persons must sign the inventory form. If an unexplained discrepancy is found, the responsible person from the old shift may be required to remain until the discrepancy is resolved or an initial investigation is conducted.

e. Since some procedures are lengthy and may extend over a shift change (e.g., system backups, system restorals, system upgrades), the role performing the action on the old shift must make sure that the same role on the new shift is aware of the progress made and of any possible problems.

f. Additional duties of the outgoing and incoming shifts include, but are not limited to, jointly:

(1) Reviewing trouble ticket actions, including the number of tickets opened, escalated, and closed. Reviewing all urgent open tickets, the current status of such tickets, and what actions must continue.

(2) Reviewing daily summary reports, component status reports, Cumulative Statistics Report (CumStat), System Status Report (SysStat), and other pertinent information and reports.

(3) Resolving station inventory discrepancies, if any.

(4) Reviewing major outages.

(5) Reviewing configuration changes.

(6) Being aware of visitors in building and any visits scheduled during the incoming shift.

(7) Calling attention to bulletins, memoranda, or other information of interest to be passed from shift to shift.

g. At the close of each shift, the Help Desk is responsible for providing a printout of all open trouble tickets requiring review for the oncoming Operations Manager.

**CHAPTER 7****INTERIM PROCEDURES****701. General**

This chapter describes Interim Procedures (IP), the need for them, and the way in which they are implemented.

DoN DMS operations and management procedures are normally contained in documents such as this one or in SOP'S developed at operational sites. But interim procedures are sometimes required to allow continued operations until component changes are made or final procedures developed. In an effort to implement DMS global system operation and management procedures, DISA has established an interim procedure promulgation process. This process ensures that operational procedures are distributed to the field as soon as they are developed to provide operational consistency. This process will also be applied to changes to procedures in previously published DISA Circulars or other formal documents pending update and distribution of the changed document.

**702. Interim Procedure Notice (IPN)**

IP'S will be provided via a GSM-issued memo under the subject title of "Interim Procedure Notice". This IPN will provide the interim procedures for a specific DMS system operation or management situation that requires coordinated and consistent response among the RNOSC'S and Navy LNOSC'S. The IPN will be sent to all the RNOSC'S, DMS Operations Working Group Members, and DMS Program Managers. The RNOSC'S will distribute the IP'S to their subordinate control centers. Recipients are urged to give widest dissemination to these procedures within their organizations. The IP'S will also be posted to the COMNAVCOMTELCOM Support Services Web Page at "[www.nctc.navy.mil](http://www.nctc.navy.mil)".

Initially, only interim procedures that apply to Navy operations will be posted to the COMNAVCOMTELCOM Web site. DMS interim procedures and operating guidelines for the USMC are under development. Once USMC procedures are in place, links to them from the COMNAVCOMTELCOM Web site will be provided. USMC sites will also have direct access to all Interim Procedure documents through the DCOC Web Page. Access controls will be in place to safe guard this information. Instructions for gaining access to the interim procedural information will be provided on the COMNAVCOMTELCOM Web site.

**703. Interim Procedure Description**

Each interim procedure will address a particular operational situation such as trouble ticketing or configuration change procedures. Each procedure will be assigned a number to uniquely

identify and reference the procedure. The procedure will also include a version number to identify and track revisions.

EXAMPLE:

IP 1-V01

IP = Interim Procedure  
1 = Procedure number 1  
V = Version  
01 = version sequence number.

The version number will be incremented each time the procedure is updated.

Every time an IPN is sent out with a new procedure or an update to an existing procedure, it will also include a list of the current procedures by IP number, version, and title. This process will ensure that all operational elements are continuously informed of the current procedures and of the applicable version. If a site does not have the current version, it is easy to reference and obtain a copy.

EXAMPLE:

Current Procedures

IP 1-V01 Operations Coordination Messages  
IP 2-V01 Message Trace Procedures  
IP 3-V01 Configuration Change Procedures  
IP 4-V01 Upgrade Procedures

#### **704. Finalizing an Interim Procedure**

The interim procedures provided in the IPN are not final and may be modified and updated as required until final publication in a DISA Circular or other DoD directive. Requests or suggestions for modification may be addressed to the GSM via an Operations Message. When a procedure is finalized and published in a DISA Circular, the procedure number will be retired.

All DMS operations activities are urged to keep the procedures on file and to comply with them as written. These procedures are developed for interoperability and operational efficiency in the global environment. This result can only be achieved if all activities participate cooperatively.

**CHAPTER 8****TROUBLE TICKET PROCEDURES****801. General**

This chapter identifies the procedures for processing and escalating trouble tickets between the Navy LNOSC'S and the RNOSC'S. It also identifies the procedures for RNOSC referral of trouble tickets to the DMS integration contractor for resolution. Figure 8-1 provides an overview of the process.

**802. Trouble Tickets**

A trouble ticket is a function of the DMS MWS. It provides the capability to record and track DMS problems from the initial report through problem resolution. When a problem can not be resolved internally, the trouble ticket can be escalated to the next level for resolution, i.e., between Navy LNOSC'S and to the RNOSC. The technical description of the trouble ticket function and operating procedures can be found in the **System Design Architecture** and the **DMS System Manual**. These documents are continuously updated and are available from the DMS Online Library. The DMS Online Library is accessible through the DISA DMS Controlled Access WEB Page. A link to DISA WEB Page is provided at "[www.nctc.navy.mil](http://www.nctc.navy.mil)". A password is required to access the site. Information on how to obtain a password is provided on the DISA DMS Web Site.

**803. Trouble Ticket Priority and User Impact**

The DMS trouble ticket priority codes and associated descriptions are identified in Table 8-1. The priority is set by the organization that originated the trouble ticket. During the initial review of the trouble ticket at the RNOSC, the priority will be validated in accordance with Table 8-1. The GSM, in coordination with the RSM, can upgrade or downgrade priorities to better meet the specified criteria. The originating Navy LNOSC will be notified if the priority is changed. The user impact will not be changed at the RNOSC.

**804. Navy LNOSC Trouble Ticket Procedures**

A Navy LNOSC will work DMS problems locally until it is determined that a problem is not within the local domain or can not be resolved with local resources. Navy LNOSC'S will contact the next upward level in the process of troubleshooting. The problem reporting and management structure for each Navy ACC is presented in Figure 8-2 through 8-5. USMC procedures parallel those of the Navy except all sites will elevate trouble ticket issues to the DCOC which will determine whether the problem should be forwarded to the RNOSC. Under Navy policy, only an ACC is authorized to contact or escalate a trouble ticket to the RNOSC. RSS'S and LCC'S will report problems and escalate trouble



tickets in accordance with the reporting structures shown. At each level, if the higher level center can not provide the necessary assistance immediately, it will advise the lower level center to prepare and escalate a trouble ticket. A Navy LNOSC-originated trouble ticket will be escalated to the next higher Navy LNOSC, until it is escalated by the ACC to the RNOSC if necessary.

Navy LNOSC escalated trouble tickets will be prepared in accordance with Table 8-2. Mandatory fields are shaded; all other fields are either automatically generated or are not applicable for Navy LNOSC escalated trouble tickets.

All troubleshooting steps taken to resolve a problem, to include system documentation references (e.g., DMS System Manual, administration guides), shall be included in the trouble ticket diary. Escalated trouble tickets without the mandatory fields and a complete troubleshooting synopsis in the diary will go into queue until the information is obtained from the submitting Navy LNOSC. If the information cannot be obtained after four business days (Monday - Friday, not including holidays), the receiving Navy LNOSC or the RNOSC will cancel the trouble ticket and send a cancellation notice by organizational message to the submitting Navy LNOSC organizational account.

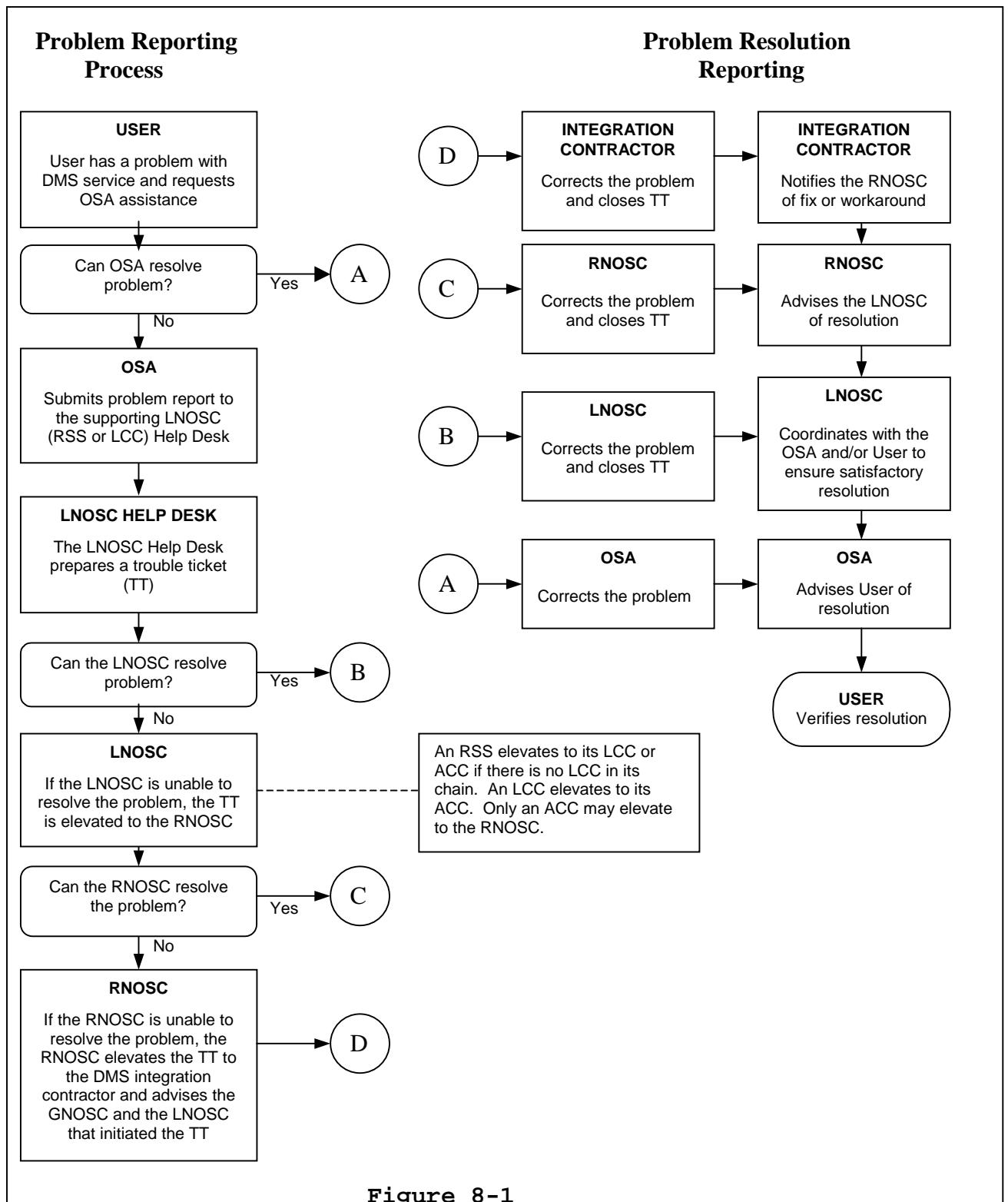
Some problems that require the Navy LNOSC'S to escalate trouble tickets may be in the DTH. When a DTH problem is known or suspected, the Navy LNOSC'S will not escalate trouble tickets to the DTH directly. The escalation chain will be followed. The RNOSC will always be the interface between the Navy LNOSC'S and the DTH and will determine whether a trouble ticket is related to a DTH problem. Requests for the status of an escalated trouble ticket will follow the same chain as the trouble ticket itself.

#### **805. Escalated Trouble Ticket Procedures**

The Navy LNOSC or the RNOSC receiving an escalated trouble ticket will process the trouble tickets according to the priority set by the originating Navy LNOSC. Processing time frames are identified in Table 8-1. The Navy LNOSC or the RNOSC will work problems until it is determined the problem can not be resolved with local resources. If the RNOSC makes that determination, it will escalate the trouble ticket to the DMS integration contractor for resolution; no other center is authorized to do so.

Each center will provide the status of open trouble tickets to the originating sites regularly. This status report includes trouble tickets escalated by the RNOSC to the DMS integration contractor.

Once a problem appears to have been resolved, the resolving center will contact the Navy LNOSC that submitted the trouble ticket to ensure the problem has been resolved. If so, the resolving center may close the trouble ticket.



**Figure 8-1**

**Problem Reporting Process Flowchart**

Rep. <sup>1</sup> Priority	Remedy <sup>2</sup> Priority	User <sup>3</sup> Impact	Criteria	Process <sup>4</sup> Time
1	Urgent	Critical	Total loss of a site's capability to provide local messaging and/or directory services, through primary <b>and</b> back-up modes or  Complete isolation from the DMS backbone for messaging and/or directory services through primary and alternate routes	24 Hours
2	Priority	Serious	Partial loss of a site's capability to provide local messaging and/or directory services through primary or back-up modes and loss of remaining capability would result in a total loss of messaging and/or directory services or  Partial isolation from the backbone through either primary or alternate routes and loss of the remaining routes would result in total isolation from the backbone for messaging and/or directory services	2 Days
3	Routine	Medium	Condition that does not cause loss of messaging and/or directory services capability with or without operational workarounds employed	4 Days
4	N/A	Low	Requests for system improvements requiring software or hardware design change or addition of a new product	Indef.
(Priority 4 is Monitor Status for RNOSC Use Only)				
Notes:				
<p>1. <u>Report Priority</u>: Reporting priority code commonly used in reports. This is not an option in the trouble ticket application.</p> <p>2. <u>Remedy Priority</u>: Priority scheme included in the Remedy Trouble Ticket application. These are the choices available to the operator. The Remedy Trouble Ticket Priorities of Urgent, Priority and Routine correspond to Report Priorities 1, 2 and 3 respectively.</p> <p>3. <u>User Impact</u>: This relates to how important the problem is to the user. It does not necessarily have to correspond to the other priorities. For example the problem is a Report Priority 3 according to the criteria but the user feels the problem is User Impact - Serious.</p> <p>4. <u>Process Time</u>: This is RNOSC processing time according to the report priority set by the Navy LNOSC.</p>				

Table 8-1Trouble Ticket Priority Table

FIELD		ENTRY
TT ID NO		Auto generated when ticket is opened
CALLER NAME		Last Name of caller reporting the problem to the ACC/LCC help desk
CALLER PHONE		Phone number of caller, Commercial and DSN if DSN is available. For overseas locations, include the international access number followed by country, city prefixes followed by the phone number.
SITE		Base, Post, Camp, Station or Region where customer is located. Organizational acronym followed by geographical location and organization
POC LAST NAME		Last name of ACC/LCC primary contact
FIRST NAME		First name and/or rank of primary contact
POC PHONE		Phone number of individual with knowledge of problem. Commercial and DSN if DSN is available.
POC E-MAIL		E-Mail address of primary contact
POC ORGANIZATION Optional		Organization acronym of primary contact. This entry should reflect the organization of individual reporting the problem at the ACC/LCC
SHORT DESCRIPTION		Primary effected equipment. Example: LDSA Problem
PROBLEM DESCRIPTION		Primary affected equipment followed by a brief description of problem. Should be short and descriptive, not to exceed 60 characters. The diary field is used in-depth descriptions. Ex: LDSA fails in directory search
SUBMITTER (Optional)		Last name of person opening the trouble ticket
ASSIGNED GROUP		N/A for ACC trouble tickets escalated to the RNOSC
ASSIGNED TO		N/A for ACC trouble tickets escalated to the RNOSC
USER IMPACT (see Table 8-1, criteria)		Critical, Serious, Medium, Low
REMEDY PRIORITY (see Table 8-1, criteria)		Priority 1: Urgent Priority 2: Priority Priority 3: Routine Priority 4: Monitor (RNOSC use only)
STATUS		
FIELD	MEANING	
New	N/A for escalated tickets	
Assigned	N/A for escalated tickets	
Auto Escalated	N/A for escalated tickets	
Work in progress	N/A for escalated tickets	
Transferred	Escalated to RNOSC	
Cancelled	N/A for escalated tickets	
Closed	N/A for escalated tickets	
Monitor	N/A for escalated tickets	

**Table 8-2****Trouble Ticket Preparation Form**

DIARY	
(1) Complete problem description	
(2) All troubleshooting steps taken to resolve a problem, to include system documentation references ( e.g., DMS System Manual, administration guides.)	
(3) Equipment time of outage	
(4) All contact with users, including date and time of failed attempts.	
(5) Format: Start all entries with "PER, name of individual providing problem description followed by location followed by description (i.e. PER Smith/Ft Monmouth LCC, SMTA WILL NOT PASS MESSAGES...//ASMITH//). Finish each entry with two slants (/), first initial, and last name// of individual entering information.	
(6) If the problem is hardware, include exact location of equipment, the CPU number of the equipment, serial number, and alternate commercial telephone numbers of the point of contact that will assist the vendor with resolution.	
HARDWARE/SOFTWARE DESIGNATION	Specify: HARDWARE or SOFTWARE
COMPONENT NAME	Identify primary equipment affected. Example: (DKMWSEFGV002)
COMPONENT POC NAME	Point of contact with knowledge of the component reported.
IP ADDRESS	Internet port address
HOST NAME (Optional)	Device hostname
PRODUCT NAME (Optional)	Product name of component
PRODUCT VENDOR (Optional)	Name of vendor supplying the product to the site
SUBMIT TO DAS	RNOSC use only
COMPONENT TYPE	Primary affected component, e.g. PGWS, BGWS, LDSA, LMTA.
HW SERIAL NO	Serial Number of hardware platform that the component resides on
DATE TRANSFERRED (D/T)	Automatic entry
OPEN TIME	Automatic entry
TRANSFER TICKET BUTTON	Used by site to transfer trouble ticket to RNOSC
CREATE DATE (D/T)	Automatic entry
TIME MODIFIED (D/T)	Automatic entry
RESOLUTION	N/A for ACC escalated trouble tickets
CLOSED DATE (D/T)	Automatic entry
CLOSED BY	N/A for ACC escalated trouble tickets
VENDOR NOTIFIED DATE (D/T)	N/A for ACC escalated trouble tickets
LMFS TSD NO	N/A for ACC escalated trouble tickets.
LMFS PTR NO	N/A for ACC escalated trouble tickets.

**Table 8-2 (Continued)**

(This form is available to OSA'S for submission of Problem Reports, including Message Trace Requests, to the LNOSC. Once made a trouble ticket, it is used by the LCC LNOSC to escalate problems to the ACC, and by the ACC to escalate problems to the RNOSC, as appropriate. Shaded fields are mandatory for ACC escalation to the RNOSC. Other fields are either automatically generated by the MWS or are not required for escalation from an ACC to the RNOSC.)

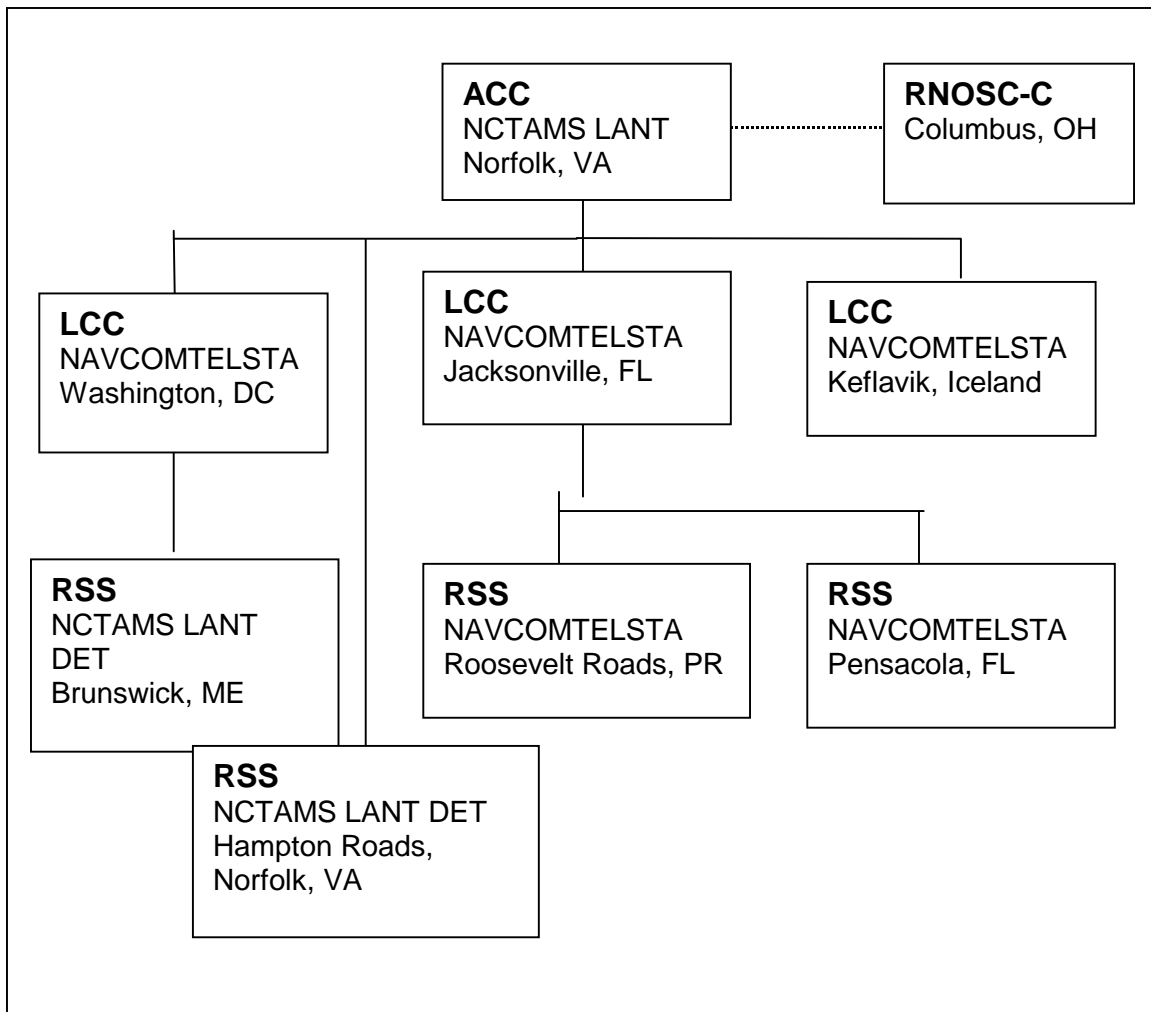


Figure 8-2

ACC NCTAMS LANT Norfolk VA Reporting and Management Structure

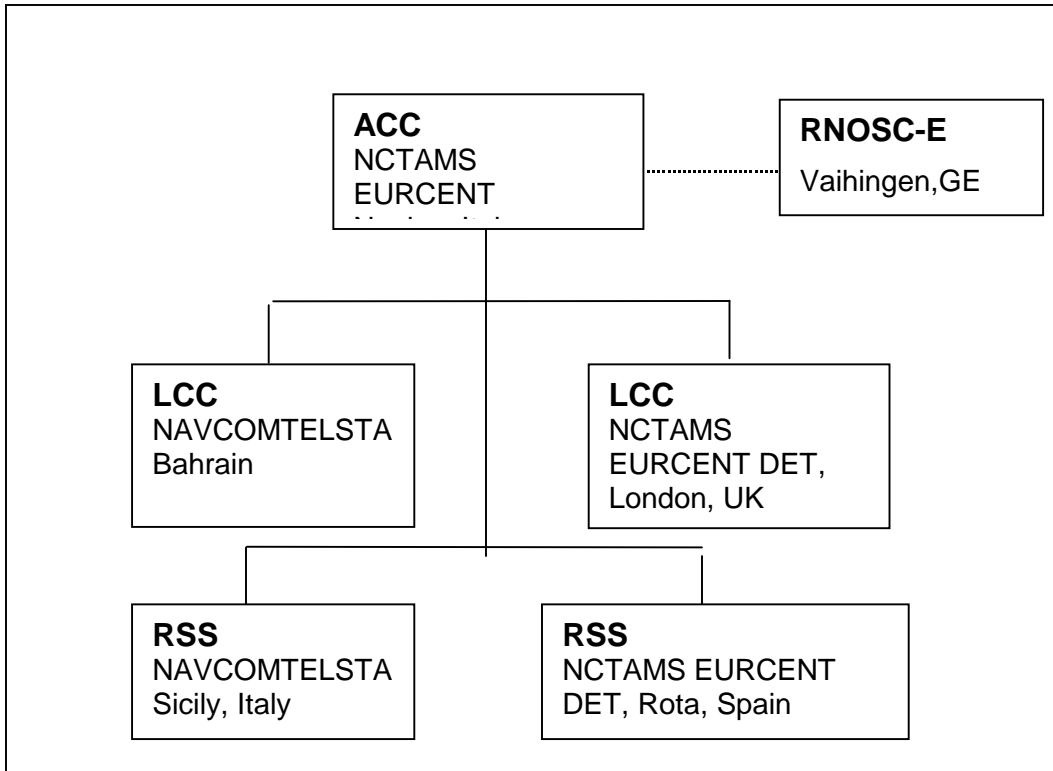


Figure 8-3

ACC NCTAMS EURCENT Naples Italy Reporting and Management Structure



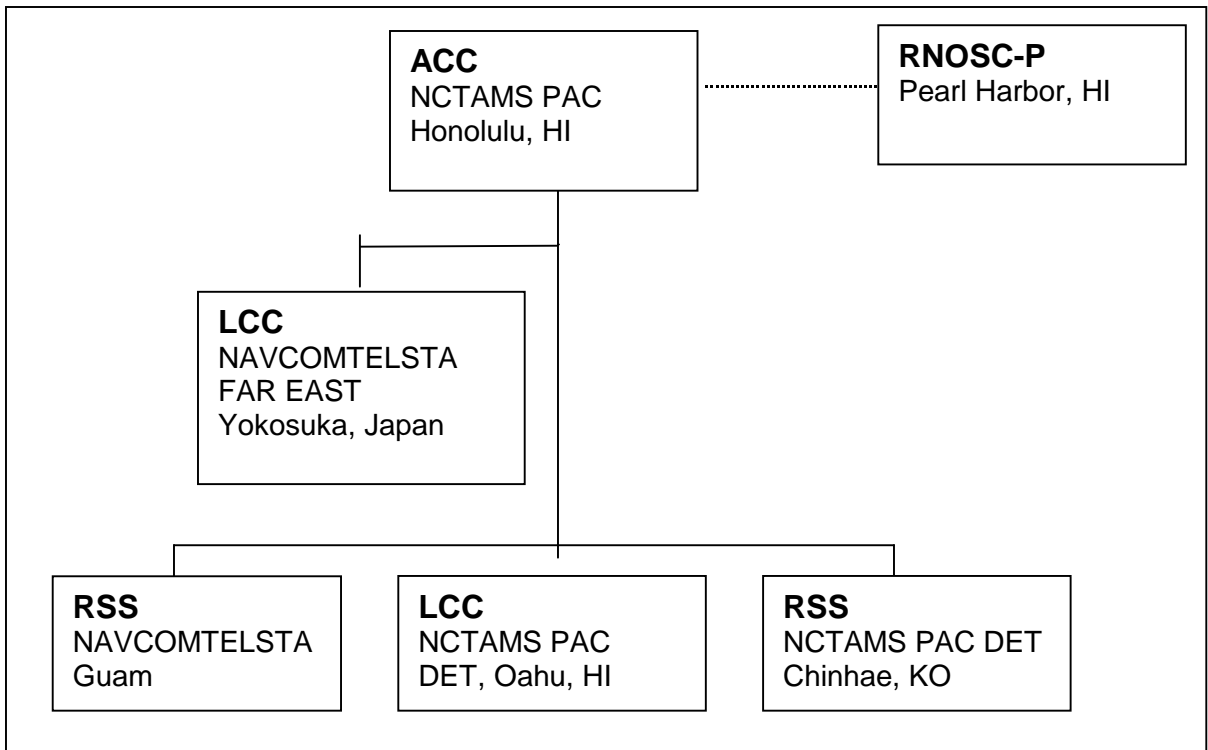


Figure 8-4

ACC NCTAMS PAC Honolulu HI Reporting and Management Structure

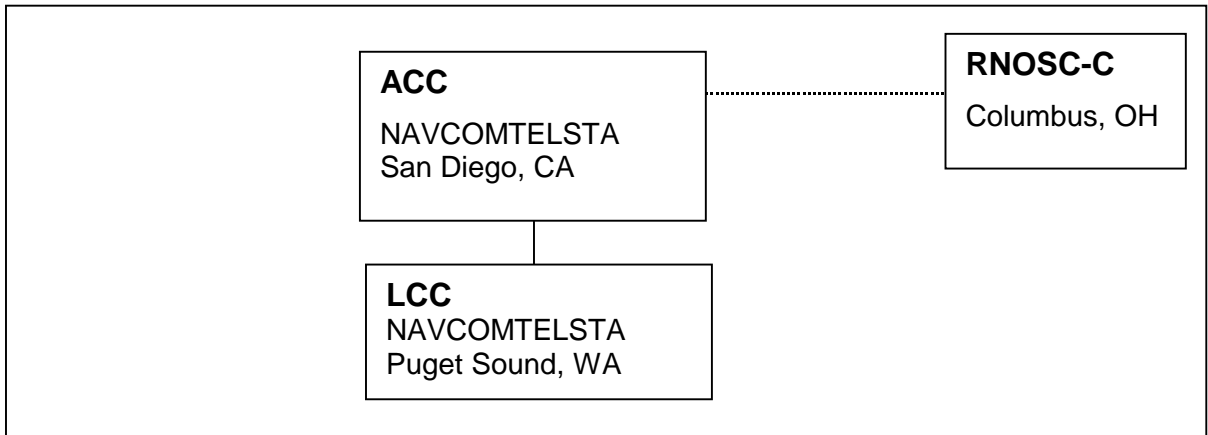


Figure 8-5

ACC NAVCOMTELSTA San Diego CA Reporting and Management Structure

**CHAPTER 9****MESSAGE TRACE PROCEDURES****901. General**

This chapter describes the message tracing process. Message tracing not only allows tracking of a single message, but provides a valuable tool in recognizing and correcting system problems.

Message tracing is usually employed when the originator and an intended recipient of a message together determine that the intended recipient did not receive a properly addressed and submitted message or that the message was received only after excessive delay. The exact means by which that determination is made and the method by which the message is identified between originator and intended recipient is outside the scope of this document. Message identification can be by date-time group (DTG), Military Message Identifier, subject matter, or any other suitable and mutually understood identification.

The actual message trace process begins with the message originator, who requests the assistance of the OSA in analyzing the problem and determining that the message was actually transmitted. If the trace must be continued outside the organization, the OSA submits a Message Trace Request (MTR) as a Problem Report to the Navy LNOSC Help Desk.

When a non-receipt is reported to the message originator, the originator has the option to resubmit the message to the recipient claiming non-receipt, to all intended recipients, or to none. If a message contained time sensitive information, its resubmission may be confusing. If the message was addressed to a Mail List of which the user claiming non-receipt is a member, the resubmission shall be directed only to that user.

**902. Message Trace Procedure**

a. Message trace requests must be submitted after the threshold times shown in Table 9-1 and within 30 days after submission of the original message. Trace requests must contain the user's message identification information, the MTS message identification, the recipient(s) to which the message is to be traced, the Message Transfer Agent (MTA) to which the message was submitted, and the time of submission. The DMS goal is to provide full response to trace requests within less than 24 hours, depending on the precedence of the original message and the availability of automated tools.

b. Message tracing is limited to the following conditions:

(1) Claim of non-receipt by an addressee without a Non-Delivery Notice being returned to the originator.

(2) Receipt of an Non-Delivery Notice (NDN) for which the cause cannot be determined.

(3) Claim of delay in receipt of a message beyond the required delivery times shown in Table 9-1.

c. Message tracing will not be used solely to receive a definitive verification of message receipt; the message originator should request such verification at the time of message transmission or by direct contact with the intended recipient.

d. An intended recipient claiming non-receipt or inordinate delay must first determine that there was no procedural failure within the receiving organization and no problem within an organizational component, such as the PUA. Once assured that the non-receipt or delay was not caused within the receiving organization, the recipient advises the originator of non-receipt. Once advised of non-receipt, the originator will ensure that there was no failure at the originating organization (e.g., failure to respond to an NDN). Having ruled out procedural error, the OSA will initiate a trace request with the serving Navy LNOSC Help Desk.

### **903. Thresholds for Message Trace Initiation**

The thresholds outlined in Table 9-1 establish the times, based on message precedence, in which a DMS message should be delivered or in which the sender should receive an NDN. If a message has not been delivered or an NDN received within the threshold, the originator can initiate a message trace according to the procedures outlined in the following sections of this document. Requests for message trace that are not in accordance with established thresholds will normally be rejected by the Navy LNOSC or RNOSC. However, operational conditions or mission-related circumstances may necessitate exceptions to the message trace policy. The RNOSC will evaluate requests for exception to established message trace policy on a case-by-case basis.

Precedence	MTS Grade of Delivery	MTS Max. Time of Delivery	Orig.-to-Recip. Max. TOD	Min. Msg. Trace Threshold	Max. Msg. Length
Critic	Urgent	3 Min.	3 Min.	30 Min.	5400
ECP			10 Min.		7000
Flash			7000		
Immediate	Normal	20 Min.	20 Min.	4 Hours	1 Mb.
Priority	Normal	20 Min.	45 Min.	6 Hours	2 Mb.
Routine	Non-Urgent	8 Hours	8 Hours	12 Hours	2 Mb.

Table 9-1

Message Trace Thresholds

**904. Lost Message**

When a trace request is completed without a determination of either message delivery or transmission of a non-delivery notice was sent, the message is considered to have been lost. If a message trace reveals such a situation, the Navy LNOSC or RNOSC Analyst must be notified. After analysis, the Analyst must submit a lost message report to the message originator, the intended recipient(s), the RSM, and the GSM. The report must indicate the nature of the message, the trace efforts involved, the time of the occurrence, and, if possible, a determination of the reason for the loss.

**905. Record Retention**

All messages originated, stored, or received in DMS are Federal Records and shall be managed in accordance with Para. 332, ACP 123 U.S. Supp. 1. All component (messaging, directory, and system management) audit trails and logs must be available on line for 30 days and off line for at least one year. On-line records must be accessible within 10 minutes and off-line records must be accessible within 4 hours. All incoming and outgoing messages must be stored at the user component (UA or MS) for a minimum of 10 days and during that time be able to be retrieved in less than 10 minutes.

a. When a user sends a message, the UA'S functionality provides accountability by assigning a Military Message Identifier (MMID) to the message and placing it in the message header. The MMID is used for local message accountability only. Once the message has been transported to the MTS via the GWS, a Message Transfer System Identifier (MTSID) is assigned to the message. The MTSID is the constant accountability number that can be used to track messages throughout the DMS global infrastructure.

b. To initiate a message trace, the OSA at the originator's organization submits a Message Trace Request as a problem report to the Navy LNOSC Help Desk. The form is shown in Figure 8-2. The Diary field is filled out as shown in Figure 9-1. This Request provides the MMID, the MTSID, and other information pertinent to the message. The LCC Help Desk makes this information the basis of a Trouble Ticket. The Help Desk operator or an MWS operator then uses the MWS to obtain the MTSID and extract all information on that MTSID from the archives of the LNOSC components. The MWS generates a report showing all action on the message. If the reason for non-delivery is found at the Navy LNOSC, the tracer action stops and all concerned are notified of the message disposition and any corrective action taken or planned.

c. If the LCC cannot fully determine if the message was successfully delivered, the LCC Help Desk forwards the MTR to the ACC for forwarding to the RNOSC for further tracking. The trace is continued through the exchange of operations messages as required. If the message was transmitted to a legacy system, the trace is continued by addressing an MTR message to the next RNOSC, the receiving LNOSC, or the legacy system service position. The originator, intended recipient, and the originating LNOSC are notified of the results at each level.

d. Message Trace Requests must be submitted within 30 days after the submission of the original message and must contain the user's MMID, the MTSID, the intended recipient(s) of the message to whom delivery was not effected, the GWS to which the message was submitted, and the time of submission. A full response to trace requests should be provided within 24 hours. If no response is received within 24 hours, a second request will be submitted. If there is no response after a second 24 hours, the submitting LNOSC will submit a third request to the DISA GNOSC (GSM) and RNOSC with an information copy to the Navy GSM. The DISA GNOSC or RNOSC shall provide a formal deposition of the message trace results.

DIARY	
(1)	Message Trace Request
(2)	Message Identification <Date-time Group> <MMID> <MTSID> <originator> claims non delivery to <intended recipient>. Research indicates message transmitted to PGWS <PGWS ID> at 041500Z Feb 00.
(3)	Request trace message and advise ALCON.

**Figure 9-1**

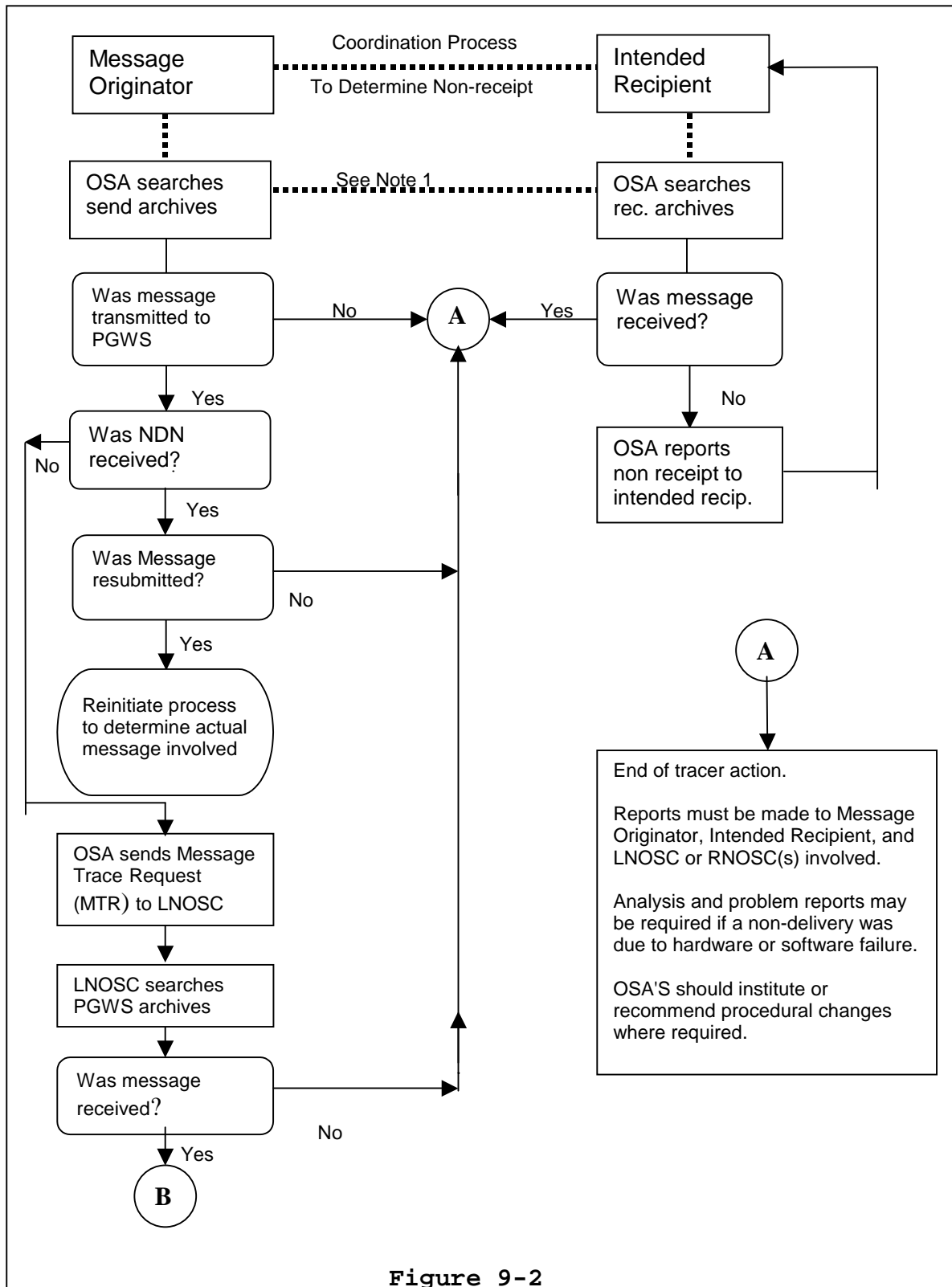
**Diary Section from Message Trace**

**906. Speed of Service Considerations**

Speed of Service is defined as the time from message submission to the time it reaches its destination UA, PUA, or MS. Table 9-1 summarizes the speed of service requirements for each message precedence at its corresponding Grade of Delivery, as specified in the Required Operational Messaging Characteristics (ROMC). Both the MTS transmission times and the originator-to-recipient times are shown. These are further qualified with maximum message sizes. The maximum message size is not the largest size message that the system will be able to carry at each level, but rather the largest size for which the indicated speed of service is required. Message length is given in bytes (or characters) of 8 bits. Total message length does not include all required system and protocol overhead. If the transmission speed cannot be met, the MTS shall deliver the message as quickly as possible. If the originator specified a latest delivery time, the message will be removed from the system and an NDN will be returned to the originator when this time is passed.

**907. Message Trace Process Diagram**

Figure 9-2 is a diagram, in flowchart form, of the message trace process. The USMC will follow a similar process. Flowchart entries for the LNOSC should be interpreted as LCC for USMC actions.



DMS Message Trace Flowchart

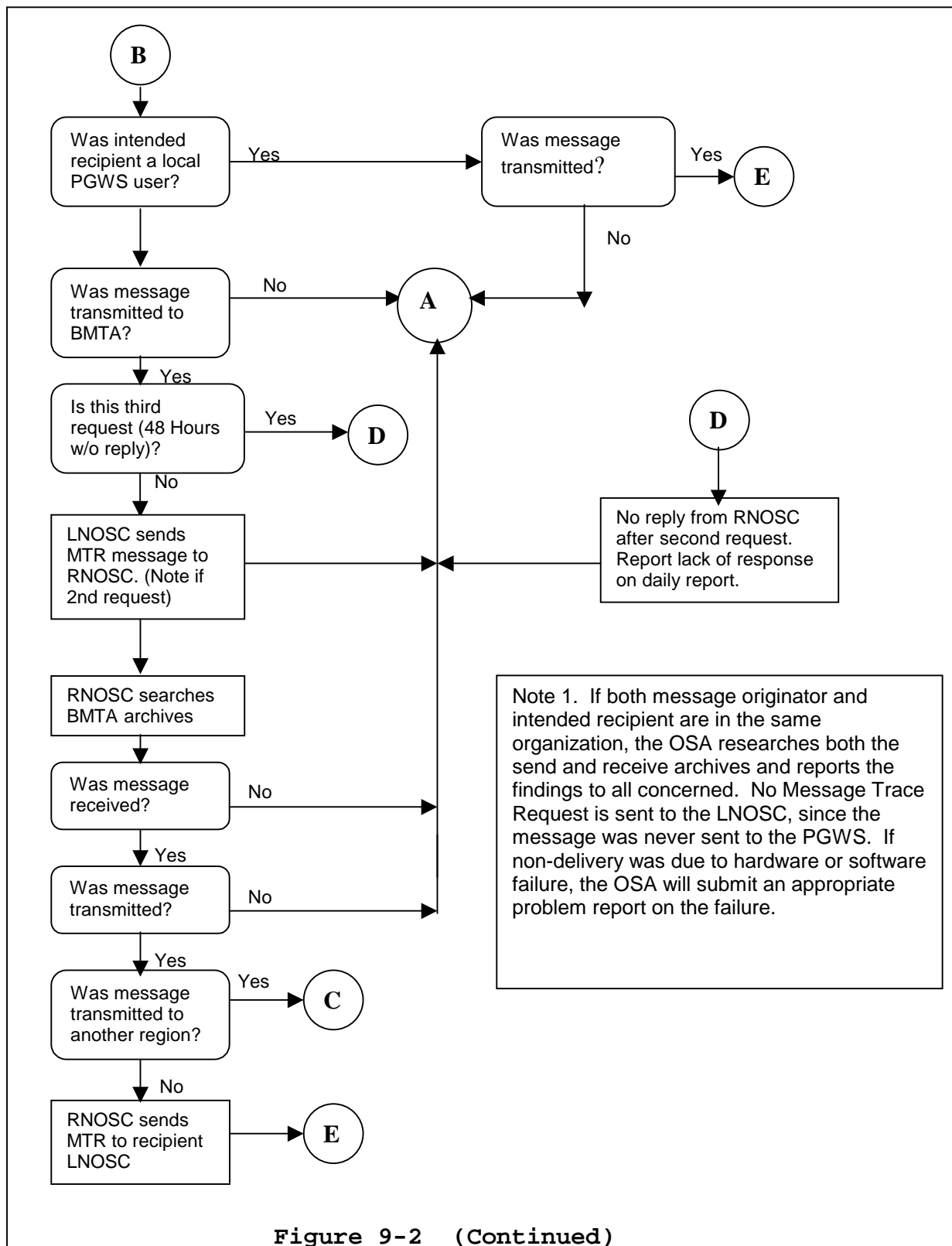
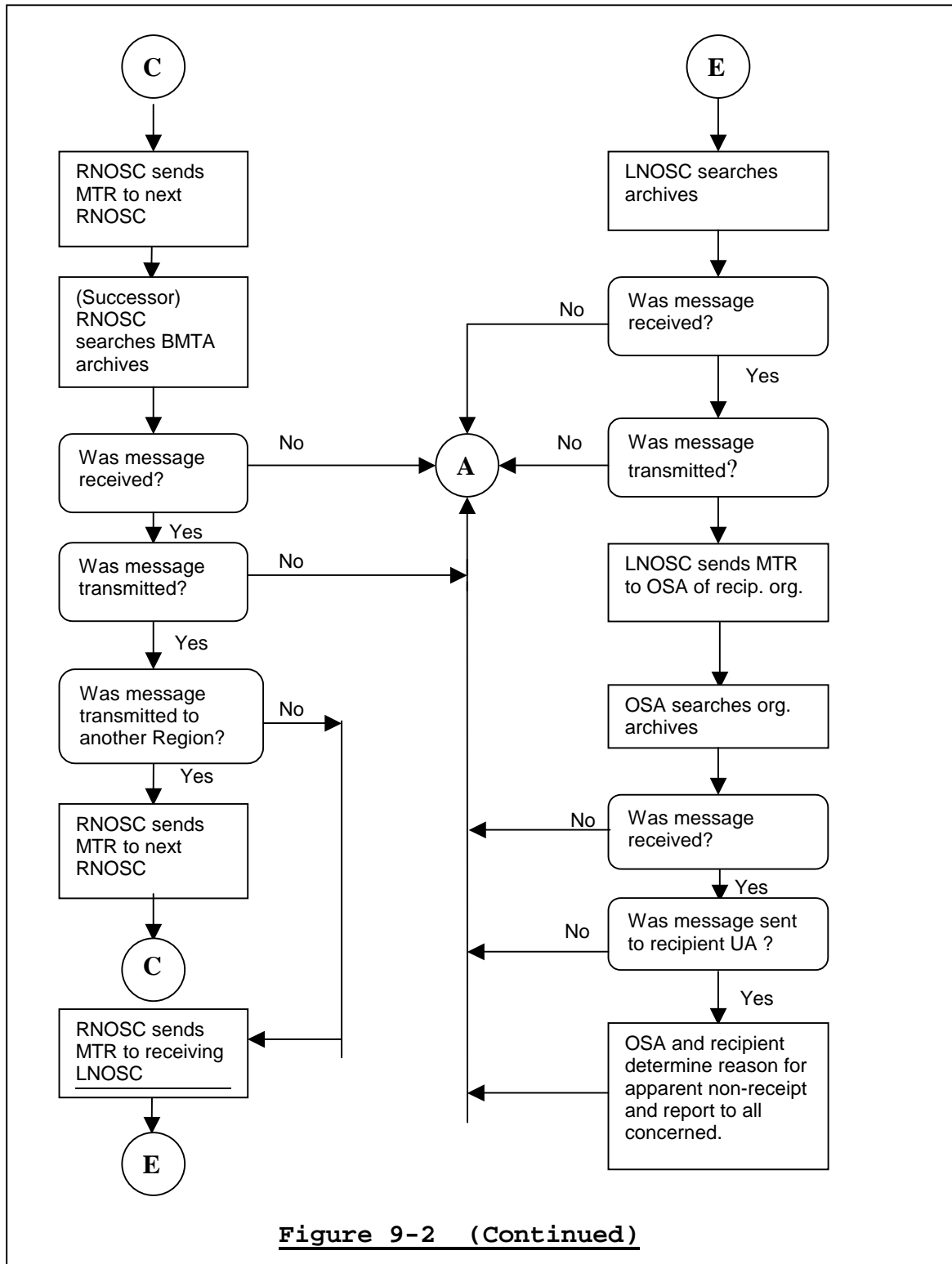


Figure 9-2 (Continued)





**Figure 9-2 (Continued)**

**908. Message Trace Scenario Example**

The scenario presented here is an example of a message trace procedure in which the message was not delivered to the intended recipient. The description of the scenario is followed by screen captures showing examples of the messages involved. Note that all message identification is for example only and, while of similar length and complexity, has no relationship to any actual message identifiers. A description of the example trace procedure follows.

a. In accordance with ACP 123 U.S. Supp. 1, all tracer action must be initiated by the originator.

b. In this hypothetical example, a message was sent from CNO to NAVAL ATTACHE LONDON. By means outside the scope of this discussion, CNO and NAVAL ATTACHE LONDON determine that the latter did not receive the message. The identification used in this determination may be the MMID, the Date-Time Group, the subject matter, or any other suitable and mutually understood identification.

c. NAVAL ATTACHE LONDON contacts his or her OSA, who searches the archives at the local GWS and PUA and determines that the CNO message was never received by the local organization. The OSA reports this finding to NAVAL ATTACHE LONDON, who then requests that the originator, CNO, begin tracer action to determine the reason for the non-receipt.

d. The CNO, as the message originator, contacts his or her OSA, who searches the archives at the originating User Agent and at any local message relay point, such as a local GWS or PUA. The OSA will also ensure that no NDN was received and ignored by the message originator. Once the OSA is satisfied that the message was properly transmitted to the PGWS, he or she originates a problem report as a message to the serving NAVCOMTELSTA Washington LNOSC. The problem report may follow a prescribed format or may be in message form as in the example. In this case as in all other problem reports, the OSA is the only role at the local organization authorized to contact the LNOSC. (Figure 9-3)

e. The CNO at this point may choose to retransmit the message to all intended recipients, to only NAVAL ATTACHE LONDON, or not to retransmit. If the data was time sensitive and no longer of value, a retransmission may be confusing to the recipient(s). If the message was transmitted to a Mail List of which NAVAL ATTACHE LONDON is a member, the originator shall retransmit the message only to NAVAL ATTACHE LONDON and not to the entire Mail List. The retransmission decision will, however, always be subject to the discretion of the message originator.

f. On receipt of the problem report at the NAVCOMTELSTA Washington LNOSC, the Operations Manager and the LNOSC OSA open a

trouble ticket for tracking purposes and log the trace request in the Message Trace Log. They then conduct a search of the PGWS and any other relevant archives. In this example, the OSA determines that the message was received and transmitted to the BMTA and the LSM. Using the information from the problem report, the OSA initiates a Message Trace Request to the RNOSC-C as in the example. While it is not shown in the examples, an LCC or RSS shall make higher level Navy LNOSC'S copy recipients on the message. (Figure 9-4)

g. At RNOSC-C, the MWS operator searches the archives of the relevant BMTA. The search finds that the message was received at the BMTA and transmitted to a BMTA at the European Regional Node. The RSM forwards the Message Trace Request to RNOSC-E to continue tracer action. (Figure 9-5)

h. At RNOSC-E, the MWS operator searches the archives of the relevant BMTA and determines that the message was received by the BMTA and transmitted to the PGWS at the NCTAMS EURCENT LNOSC in London. The RSM forwards the Message Trace Request to that LNOSC, with a request to continue the trace. (Figure 9-6)

i. At the NCTAMS EURCENT LNOSC, the OM and the OSA search the archives of the relevant PGWS. The archives and records indicate that the PGWS failed after the time of receipt of the message and had to be rebooted. Messages in the PGWS system at the time could not be recovered. Depending on the circumstances, the OM may open a trouble ticket to report the lost message in addition to the trouble ticket already opened on the PGWS failure. The LSM responds to the Message Trace Request with a description of the problem that resulted in non-delivery of the message. (Figure 9-7)

j. On receipt of the message from NCTAMS EURCENT LNOSC, the NAVCOMTELSTA Washington LNOSC closes the trouble ticket and closes the Message Trace Log entry. The trace message from NCTAMS EURCENT was addressed to the originator of the traced message, CNO. The serving LNOSC personnel will be available to respond to any further questions from CNO.

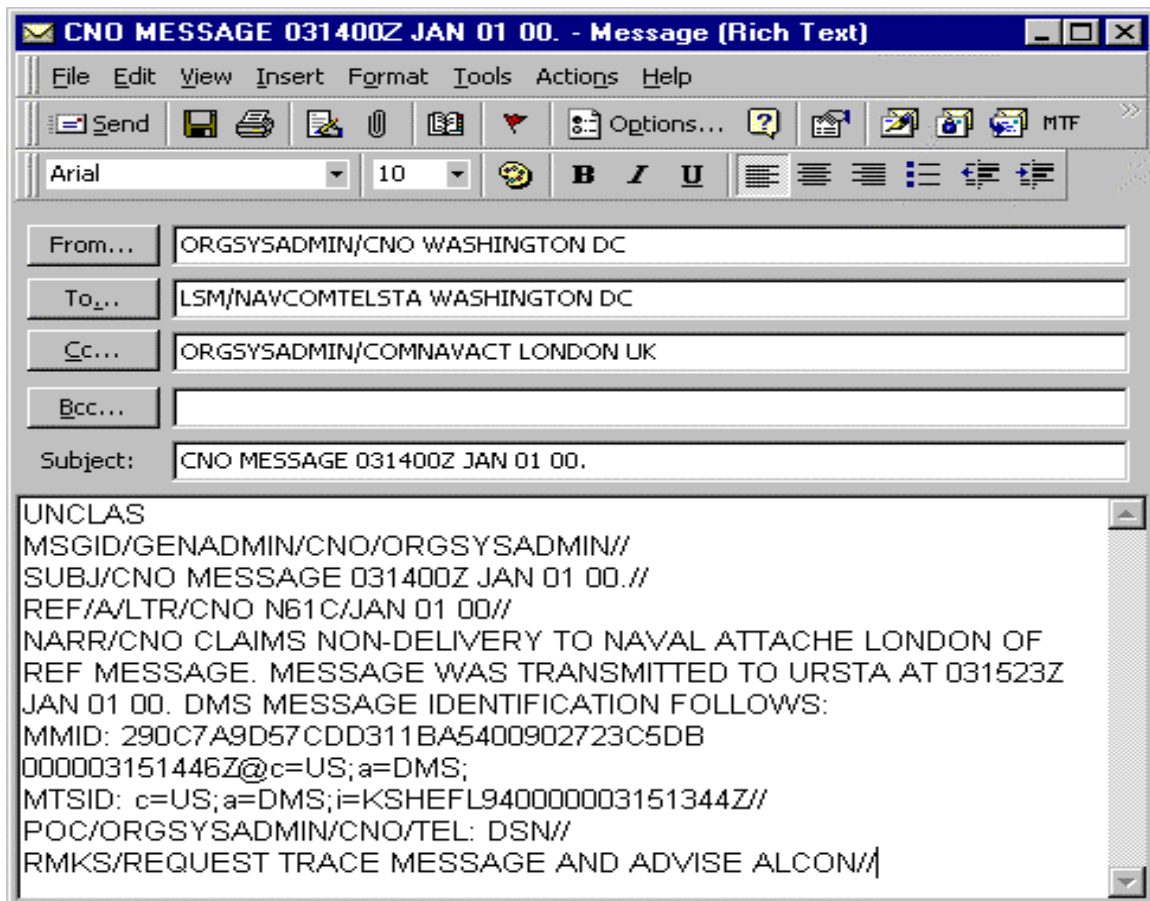


Figure 9-3

Message from Originator Organization to LNOSC

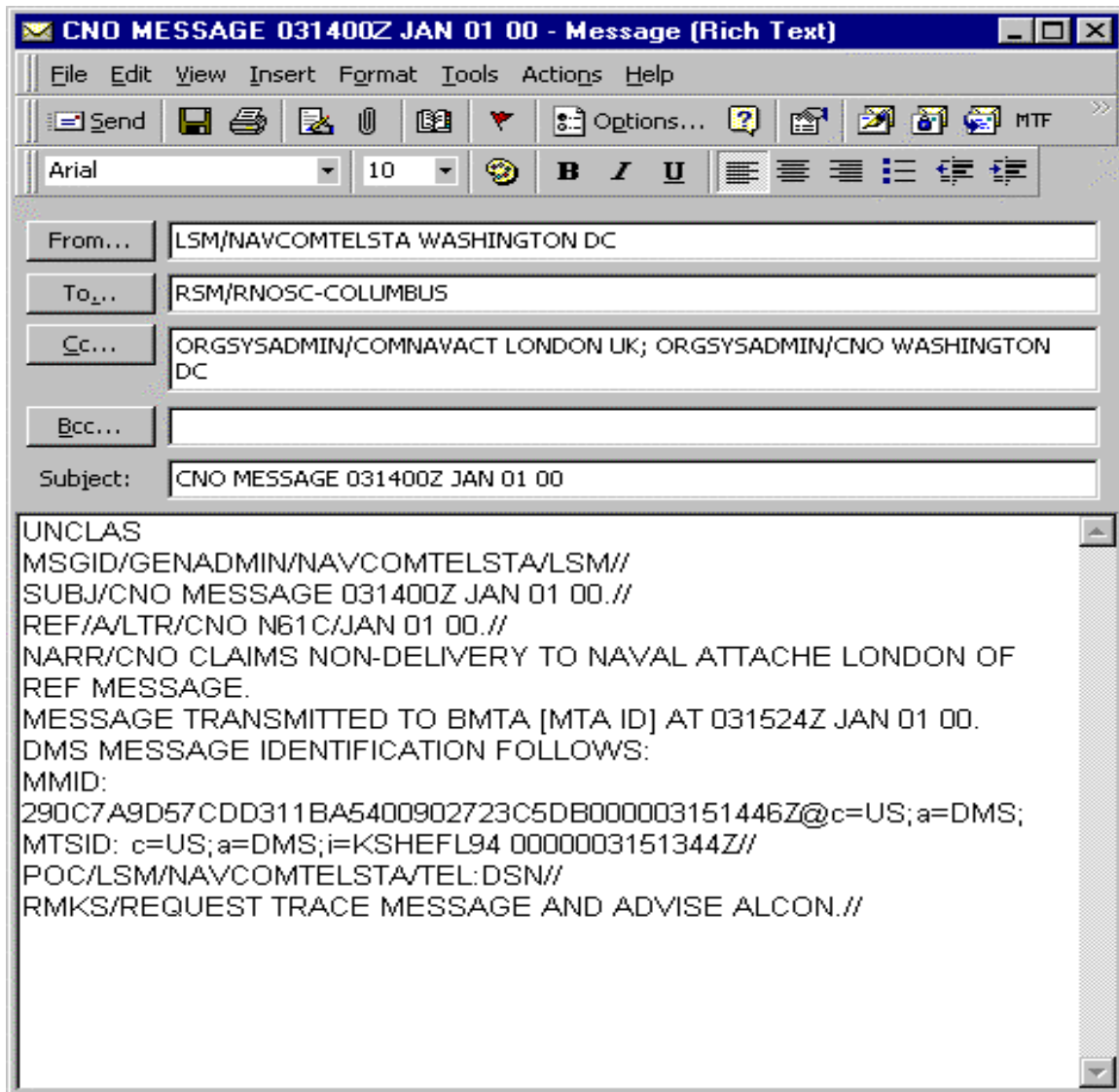


Figure 9-4

Message from the LNOSC to RNOSC-C

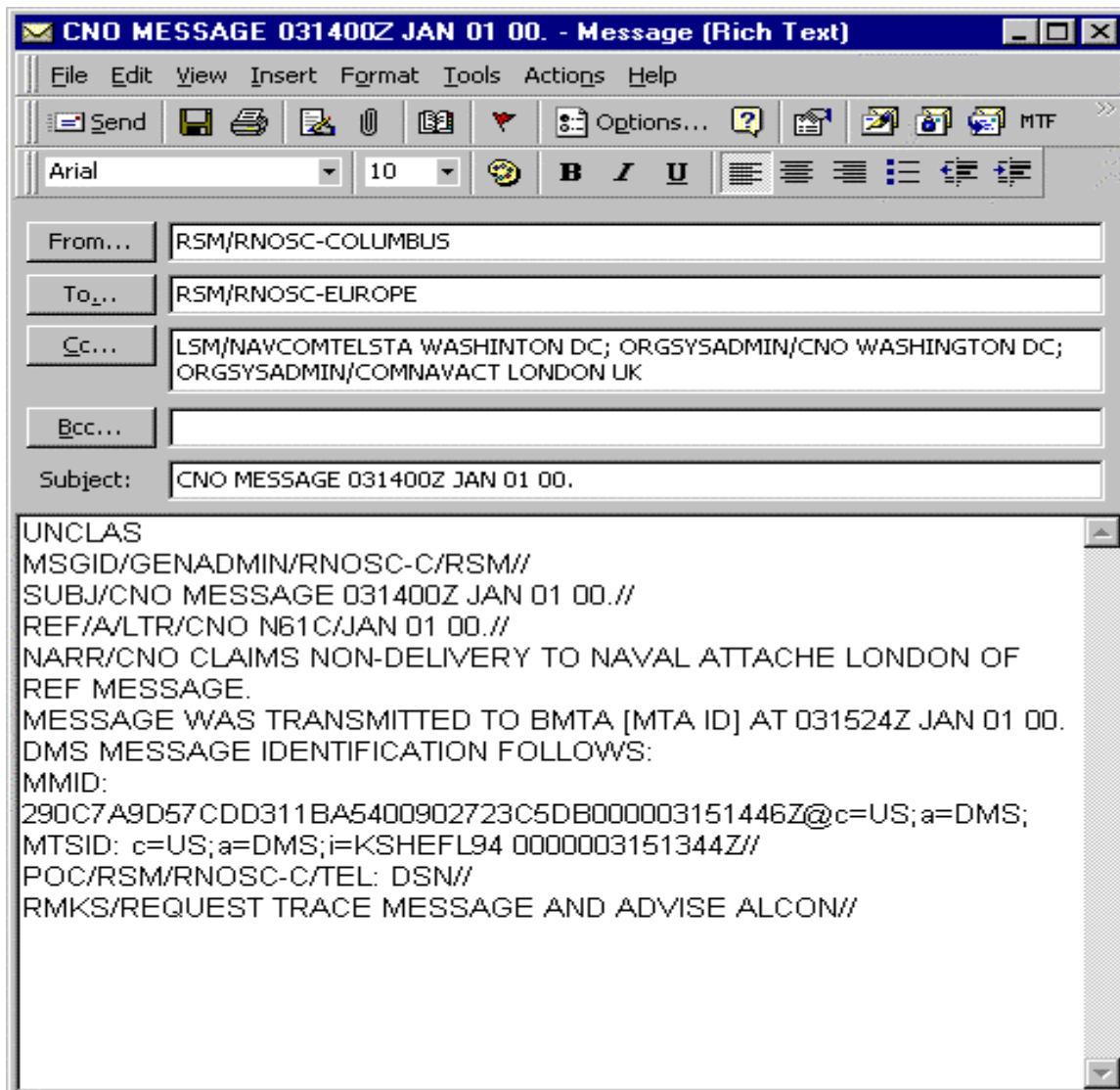


Figure 9-5

Message from RNOSC-C to RNOSC-E

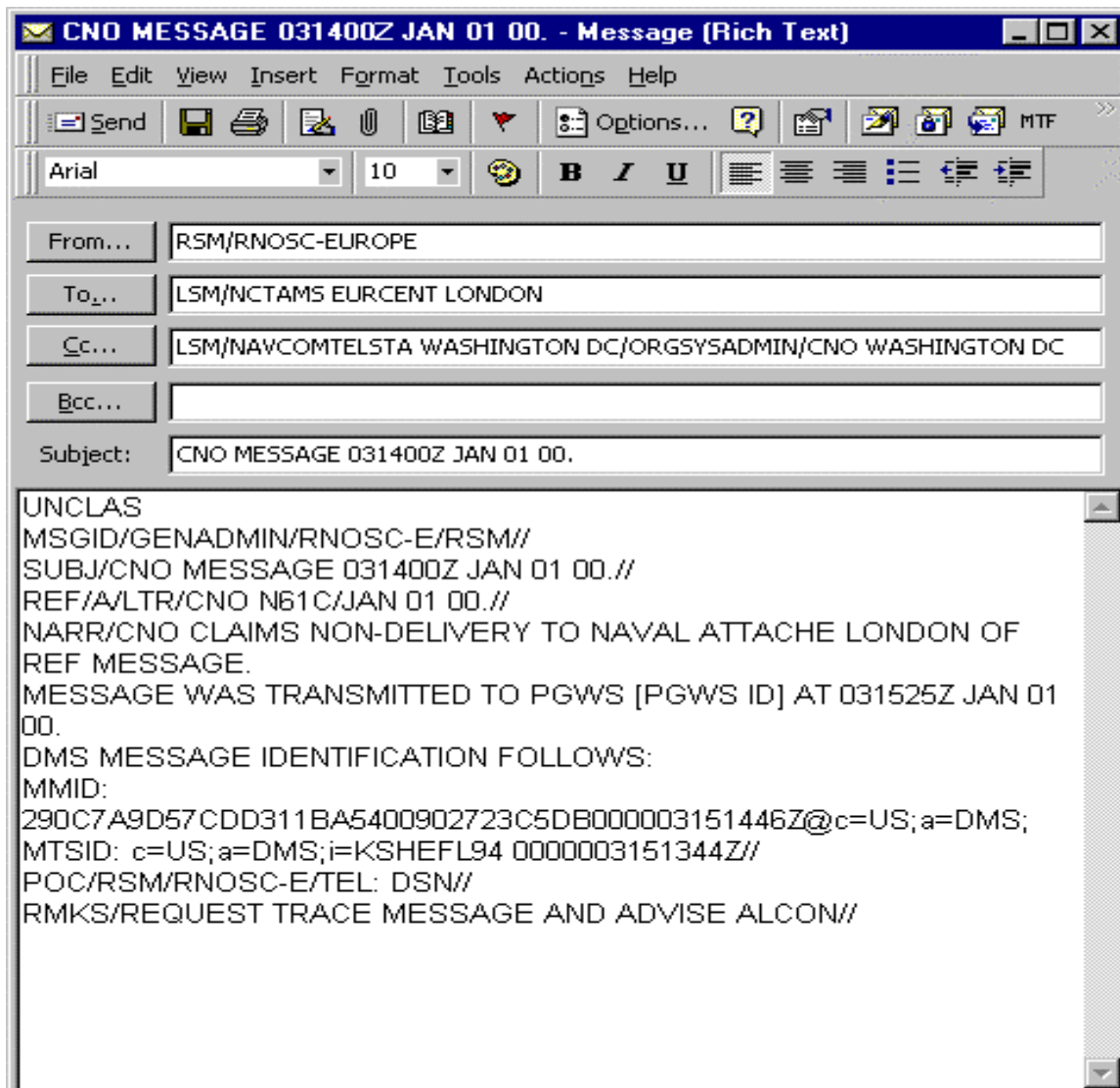


Figure 9-6

Message from RNOSC-E to Recipient's LNOSC

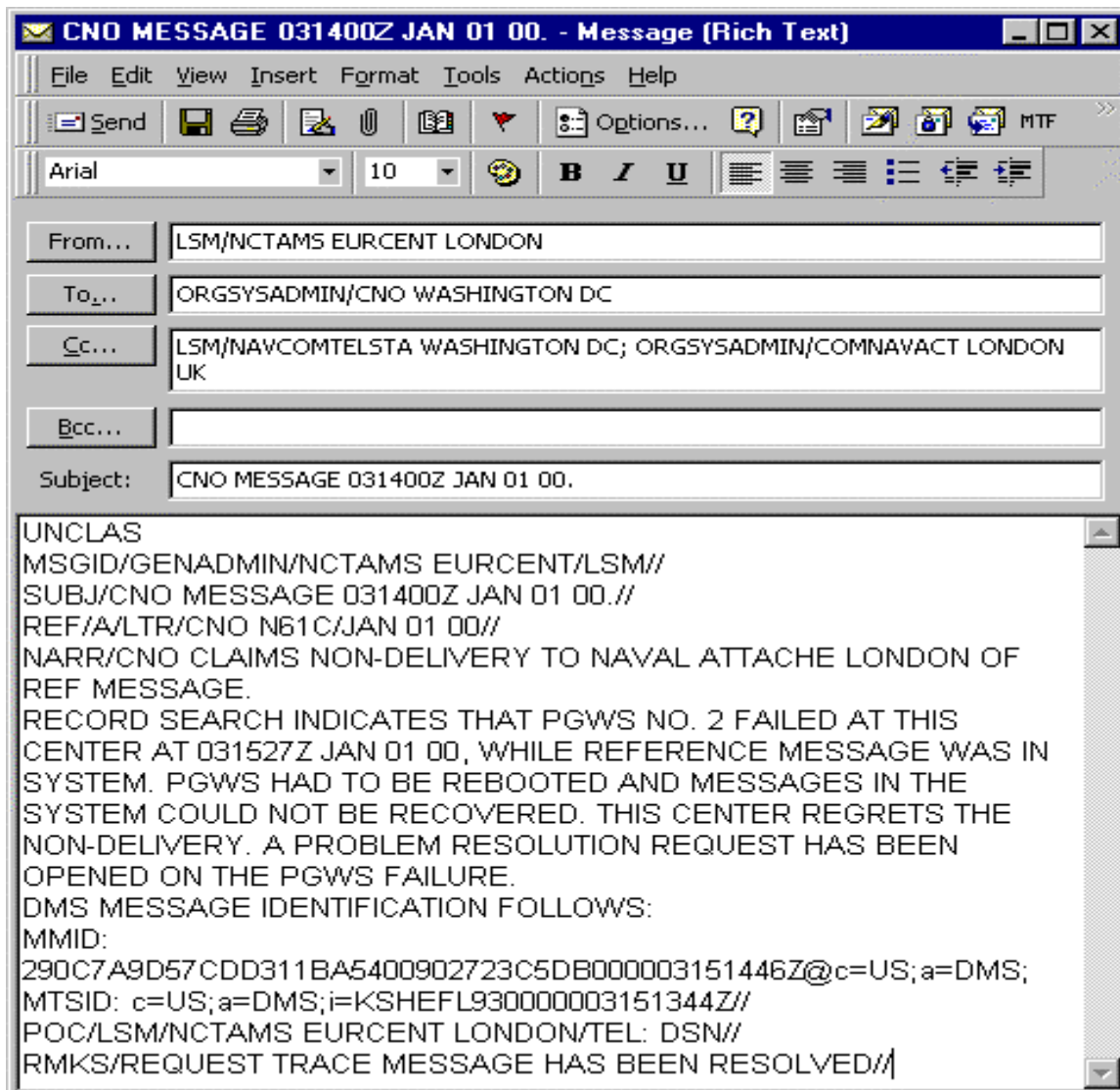


Figure 9-7

Message from Recipient's LNOSC to All Concerned



**CHAPTER 10****SOFTWARE PATCH PROCEDURES****1001. General**

This chapter provides policy and procedures for the distribution, documentation, and implementation of interim software changes (or "patches") for the DMS.

**1002. Policy**

The DMS GSM will authorize the distribution and installation of software patches for DMS components. A patch is an interim update to the program baseline pending a new software release. It is an actual piece of object code that is inserted into (patched into) an executable program. Microsoft service packs are also considered as a patch for the purposes of this document. DMS system operation managers (RSM, ASM, LSM) will only allow installation of GSM-authorized patches. Patches acquired by any other means, such as from commercial software vendors (from a web site or otherwise), are not authorized.

**1003. Evaluation and Testing**

All software patches will undergo evaluation by the DMS integration contractor in the integrated DMS environment to ensure the patch is compatible with the currently fielded DMS system. Further testing is conducted by the Joint Interoperability Test Center (JITC) for Functionality, Interoperability, Security, and Performance (FISP).

**1004. Field Engineering Notice (FEN)**

The DMS FEN is the primary means of providing to OSA'S and operators the assistance and instructions needed for implementation, sustained daily operation, and maintenance of one or more DMS components or associated software. A FEN is normally prepared by the DMS integration contractor and approved by the GSM before it is disseminated. FEN'S are numbered sequentially and continue indefinitely. The FEN number is the identifier to use when referring to a FEN. Following successful FISP testing, the GSM will approve the patch and issue a FEN to distribute the patch software to the RNOSC'S, Navy LNOSC'S, USMC LCC'S, and DTH'S. The FEN will also contain installation instructions and patch documentation. The DMS GSM will specify a date and time by which the patch must be installed.

**1005. Defense Information Infrastructure (DII) Asset Distribution System (DADS) Posting**

The FEN containing the approved patch will be posted to the DADS. The DADS is a client/server application on the World Wide Web used to securely distribute DISA DMS assets. A link to the

DADS home page is provided through the "[www.nctc.navy.mil](http://www.nctc.navy.mil)" Web Page.

Registration and user procedures are available at this URL. Note: The DADS uses Secure Sockets Layer (SSL) encryption to protect transmitted information. Users who access this site must have a signed certificate associated with their Internet browser.

#### **1006. Patch Notification**

The GSM will notify the CONUS, Europe, and Pacific RNOSC'S that the new FEN has been posted. The RNOSC'S will notify the Navy LNOSC'S in their AOR via organizational message to download and install the patch from the DADS. The RNOSC'S will identify the GSM designated deadline for installing the patch in the notification.

#### **1007. DoN Distribution Requirements**

The DoN has chosen to implement a centralized approach for distribution of patches and has identified that requirement to the DMS GSM and the RNOSC'S. For DoN distribution, the RNOSC'S will send FEN notifications to each Navy LNOSC and USMC LCC in their AOR, but Navy LNOSC'S and USMC LCC'S will not implement a FEN until directed by the Navy GSM or USMC DCOC.

#### **1008. Distribution of Large Patches**

Large patches may be disseminated independently of DADS because they can not be efficiently downloaded. In these situations, the GSM will determine the method of patch distribution and will advise the RNOSC'S accordingly. The RNOSC'S will in turn advise the Navy LNOSC'S in their AOR.

#### **1009. Navy LNOSC Patch Installation**

Navy LNOSC'S must obtain COMNAVCOMTELCOM approval before applying patches to Navy components. The Navy LNOSC System Administrator (SA) for the affected component will pull the patch from the DADS server via the Internet, prepare the patch for installation, and await direction. If such direction is not received in a timely manner (dependent on installation instructions), the SA must advise COMNAVCOMTELCOM that the patch is ready and request approval for installation. Once COMNAVCOMTELCOM approval is received, the SA will perform the installation according to the instructions provided in the FEN.

The Navy LNOSC will open a trouble ticket prior to installing the patch. The Short Description and Problem Description will clearly identify the FEN number associated with the patch. The Navy LNOSC will record the patch installation events in the diary of the trouble ticket. Events will include the installation start and stop times and any significant events or problems encountered during the installation. Upon successful completion

of the patch installation, the Navy LNOSC will enter "FEN <number>, Patch <title>, successfully installed on <date>" in the diary. The Navy LNOSC will then escalate the trouble ticket to the RNOSC.

#### **1010. Patch Installation Problem Resolution**

If problems are encountered in the patch installation that the Navy LNOSC cannot resolve, the Navy LNOSC will prepare a trouble ticket and escalate it to the RNOSC. If the RNOSC can not resolve the problem, the RNOSC will forward it to the DMS integration contractor for resolution. The site will open a separate trouble ticket for each problem encountered during the patch installation. The trouble ticket Short Description and Problem Description will identify the FEN number associated with the patch and clearly state that the problem is associated with the patch installation. This procedure enables a clear audit trail of the problem and its relationship with the patch. All patch installation problems will also be identified in the trouble ticket diary opened per Paragraph 1009. The diary entry will include a summary of the problem, the problem resolution, and the trouble ticket numbers.

#### **1011. Reporting**

##### **1011.1 Navy LNOSC Reporting**

The Navy LNOSC escalation of a trouble ticket announcing the successful installation of a patch satisfies the Navy LNOSC reporting requirements. Navy LNOSC'S must also notify COMNAVCOMTELCOM of patch installation and of any problems encountered via an organizational message.

##### **1011.2 USMC LCC Reporting**

USMC LCC'S escalation of a trouble ticket announcing the successful installation of a patch satisfies the LCC reporting requirements, but USMC sites must also notify the DCOC of patch installation and any problems encountered via an organizational message.

##### **1011.3 RNOSC Reporting**

Each RNOSC will provide a daily patch status report to the GSM for each patch that is issued. The report format will be identified by the GSM.

#### **1012. Overdue Patch Installation**

Failure of a Navy LNOSC to install a patch by the required date could result in disruption to the global system. If this should occur, the GSM may terminate DMS service to the delinquent site. Service termination may remain in effect until such time

as the required FEN or patch is in place and operational. The GSM will notify the Service or Agency's sustaining command prior to terminating service.

#### **1013. USMC Patch Installation**

USMC sites must obtain DCOC approval before applying patches to local components. DCOC will pull the patch from the DADS server via the Internet and distribute it to the individual sites. Sites will open trouble tickets with the servicing RNOSC. Successful completion of the patch installation will close the trouble ticket. Problems will be escalated to the RNOSC for resolution. The DCOC will be kept informed of all trouble ticket actions to include issues or problems that required escalation to the RNOSC and notification upon completion of the task.

**CHAPTER 11****SYSTEM UPGRADE PROCEDURES****1101. General**

This chapter provides the operational transition procedures for upgrading the global DMS system (both infrastructure and Navy LNOSC areas) with new product releases.

**1102. Scope**

These policies and procedures apply to all future DMS releases. They are applicable to the RSM'S, the ASM'S, and the LSM'S. This chapter provides the operational procedures necessary to execute the Implementation Strategy and Plan (ISP) for DMS Releases prepared by the DMS integration contractor.

**1103. Overview****1103.1 DMS Product Releases**

DMS implements and deploys enhanced system software capabilities through a series of coordinated software product releases. Each release of DMS provides new capabilities and/or enhancements to established products as part of an integrated system. Release levels also correspond to achievement of significant program capabilities.

A major software release can be expected approximately every six months. This maintains momentum and permits infusion of new technology on a routine basis. The DMS integration contractor uses the DMS Configuration Control Board (CCB) approved capabilities matrix to work with product providers to develop an integrated product plan for each release.

The DMS Product Plan document explains the DMS product development and release process in more detail. The DMS Product Plan is available for download from the on-line library from the DMS Controlled Access Web Page at "[www.disa.mil/d2/dms](http://www.disa.mil/d2/dms)".

**1103.2 DMS Implementation Strategy and Plan (ISP) for DMS Releases**

The ISP is prepared by the DMS integration contractor at the direction of the DISA DMS Program Manager (PM). It defines the strategy, procedures, and schedule for the implementation of a new DMS product release. The ISP will be published and released concurrent with JITC integration testing and prior to Beta Site testing. The ISP is available on the DISA DMS Controlled Access WEB page in the On-line Library. All personnel involved in the implementation of DMS Product Releases should become familiar with the ISP. The ISP provides detailed information on all

aspects of the release and its implementation that is of concern to all staff levels. The information and procedures in the following paragraphs serve as guidelines for executing the information in the ISP.

#### **1104. Operational Impact**

In the global DMS operational environment, it is not possible for all sites to complete the transition to a new product release simultaneously. Consequently, DMS product releases are, to the extent possible, developed to be backward compatible with the previous release, facilitating interoperability and coexistence of two releases for a period of time. The Transition Strategy section in the ISP addresses the capability of the release for backward compatibility and provides a transition plan that will minimize the impact on the operational environment. The ISP also includes a chapter that identifies the risks associated with the upgrade and the mitigation strategy to alleviate these risks. The GSM will assess the operational impact of the release and, if necessary, provide supplemental procedures to complement the transition strategy in the ISP. The Services and Agencies and ASM'S and LSM'S should also determine the operational impact of the product release on their DMS ACC and LCC operations and plan accordingly.

#### **1105. Transition Procedures**

The DMS GSM, in conjunction with the DISA DMS Program Manager, will authorize release of a new DMS product when the product has satisfactorily completed testing and meets established criteria. The ISP identifies the strategy to transition the DMS network (infrastructure and ACC and LCC sites) to the new product release version.

#### **1106. Transition Schedule**

The ISP identifies the order of upgrade. The order of upgrade identifies the sequence in which infrastructure (RNOSC, Regional Node, DMS Transition Hub), Beta test, and Navy LNOSC sites will be upgraded. In line with the order of upgrade, the ISP provides the schedule that sites will upgrade. The GSM will assess the operational impact of the schedule. If necessary, the GSM will provide additional scheduling instructions to the RNOSC'S and to the Services and Agencies. The Services and Agencies should review the ISP schedule for local planning purposes. If there are any conflicts, the Services and Agencies will notify the DMS GSM to resolve the conflict. The "official" schedule is provided by the GSM.

#### **1107. GSM Authorization to Install**

The DMS GSM will send out a notification authorizing sites to install the new product release. Navy ASM'S and LSM'S should not install the new product release until authorization has been

received from COMNAVCOMTELCOM. USMC sites will be notified via the DCOC. The DMS GSM notification may be distributed by a DMSSTA message or by a DMS Operations Message to the RNOSC'S Operations Accounts. The RNOSC'S will notify the Navy LNOSC'S via Operations Message to the Navy LNOSC Operations Accounts. Navy policy is that Navy sites will not install a new release until directed by COMNAVCOMTELCOM. USMC policy is that USMC sites will not install a new release until directed by the DCOC. To ensure that there are no compatibility problems, COMNAVCOMTELCOM and DCOC may direct one or more sites to implement the release prior to general installation. All actions at USMC sites will be coordinated by the DCOC.

#### **1108. Software Distribution**

The new product release will be distributed to sites in a phased approach according to the order and schedule for the upgrade. The software, complete with installation instructions and documentation, will be shipped to commissioned sites by the DMS integration contractor. The list of documentation for the new release is identified in the ISP. Software will be distributed to the various engineering activities (contractor and Service and Agency) for staging and configuring and to sites in the process of installation at the time of transition. The ISP contains a table with the list of sites to receive the software and their addresses. This list should be reviewed closely and any discrepancies identified to the DMS integration contractor Trouble Desk to resolve the discrepancy.

Software will normally be received by the sites in advance of the upgrade schedule, but must not be installed at Navy sites until the DMS GSM authorization and COMNAVCOMTELCOM direction are received. USMC sites will await DCOC direction. Sites that do not receive their software should contact their servicing RNOSC.

#### **1109. Upgrade Status Ticket**

The Beta sites and Navy LNOSC'S shall open a DMS Upgrade Status Ticket when they begin the upgrade process. The DMS Upgrade Status Ticket is a trouble ticket prepared to track and report the status of the upgrade process to the servicing RNOSC. The Beta sites and Navy LNOSC'S shall submit the Upgrade Status Ticket 72 hours prior to beginning the upgrade. The Upgrade Status Ticket will identify the start of the upgrade process and the proposed schedule for executing each step in the process.

If the upgrade testing requirements involve backbone testing with the RNOSC, the projected backbone testing schedule will be included in the status ticket. If the backbone testing schedule is in conflict with other RNOSC activities, the RNOSC will work with the site to reschedule backbone testing.

The ASM or LSM will update the trouble ticket periodically as the upgrade progresses. The updates will identify the start and

completion of each step in the process. When the upgrade process requires taking site components connected to the backbone offline, the ASM or LSM will notify the RSM via Operations Messages of the time the component is removed from and restored to service. This procedure ensures that the RSM is aware of the status of site components connected to the backbone.

The RSM will close the Upgrade Status Ticket when the site notifies the RSM that the verification test procedures were executed successfully.

The DMS Upgrade Status Ticket will not be used for problems encountered during the upgrade. When a problem is encountered, a separate trouble ticket will be opened for each problem and processed according to established procedures; the trouble ticket must clearly indicate the product release designation (e.g., 2.2). A separate trouble ticket is required to effectively track each problem as it is escalated from the site to the RSM and to the DMS integration contractor.

#### **1110. Site Specific Upgrade Procedures**

##### **1110.1 RNOSC, Regional Node, and DTH Upgrade Procedures**

The RSM will monitor DMS Upgrades at Regional Nodes and DMS Transition Hubs. The RSM will coordinate the upgrade schedule and implementation with the personnel performing the upgrade (i.e. System Administrator, contractor, or other). The RSM will open a DMS Upgrade Status Ticket when a Regional Node or DTH begins to perform the upgrade.

The DMS integration contractor will provide the RSM'S technical support to assist in the transition at the RSM'S, Regional Nodes, and the DTH'S to include the following:

- a. On-call installation support.
- b. On-call troubleshooting.
- c. Testing assistance to ensure proper operation of infrastructure components.

The RNOSC should contact the DMS integration contractor trouble support desk for this support.

The RNOSC will ensure verification test procedures described in Paragraph 1114 are performed. When the upgrade process is completed, including successful verification testing, the RNOSC will close the Upgrade Status Ticket.

##### **1110.2 Beta Test Site Upgrade Procedures**

The Beta sites will receive the DMS release approximately two weeks after the release has been delivered to JITC for



integration testing. Beta sites are required to execute a series of test procedures against the release to verify correct operation. They are also required to provide a weekly status report on their test progress and issues. The test and weekly status report procedures can be found in the Transition Strategy chapter of the ISP under Beta Sites.

The Beta site may upgrade to the new release when it has received authorization from the Navy GSM or USMC DCOC. The Beta site will initiate the upgrade process by preparing a DMS Upgrade Status Ticket. The Beta site will upgrade components according to the order of upgrade recommended in the ISP.

When Beta test sites require technical support, they will prepare a trouble ticket that clearly states that the problem is with Beta software. A separate trouble ticket is required for each individual problem identified. The trouble ticket(s) will then be escalated to their servicing RNOSC. The RNOSC will briefly review the trouble ticket and if they are not able to resolve it rapidly, they will escalate the trouble ticket to the DMS integration contractor technical support desk for resolution.

The Beta site will conduct the verification test procedures described below. When the entire site system upgrade is complete, the Beta site will close the DMS Upgrade Status Ticket and forward it to the RNOSC notifying them of completion of the site upgrade.

#### **1111. Upgrade Procedures**

Navy LNOSC'S will implement DMS System upgrades after authorization is received from the DMS GSM, either by DMSSTA message or by Operations Message from the RNOSC, but not until directed to do so by COMNAVCOMTELCOM. USMC sites will receive authorization from the DCOC.

The Navy LNOSC will initiate the upgrade process by preparing a DMS Upgrade Status Ticket. The site will upgrade components according to the order of upgrade recommended in the ISP. The Navy LNOSC sites will utilize the standard process for receiving technical support through escalating Trouble Tickets to their servicing RNOSC. If the RNOSC is not able to resolve the issue, it will escalate the Trouble Ticket to the DMS integration contractor trouble desk for resolution. Any problem reports directly from a Navy LNOSC to the DMS integration contractor trouble desk will be directed back to the appropriate RNOSC for its action. The DMS integration contractor and the RNOSC'S will work closely together to identify any systemic issues or trends and communicate these to the sites.

The Navy LNOSC will perform the verification test procedures described below. When the entire site upgrade is complete and tested, the site will close the DMS Upgrade Ticket and forward it to the RNOSC to notify them of completion of the site upgrade.

The Navy LNOSC will also notify COMNAVCOMTELCOM by organizational message when the upgrade is complete. USMC sites will notify the DCOC.

#### **1112. System Upgrade Reporting**

The RNOSC'S will report the status of the DMS Upgrade progress in their AOR through the RNOSC DMS Daily Status Report to the GSM. This includes the status of Regional Nodes, DTH'S, Beta Sites, ACC'S, and LCC'S. Navy LNOSC'S will also report the upgrade status to COMNAVCOMTELCOM by organizational message to the COMNAVCOMTELCOM account. USMC sites will report to the DCOC.

#### **1113. DMS Upgrade Completion**

The DMS System Upgrade will be completed when all the operational sites upgrades have been declared complete through the upgrade status ticket and reporting process described above. Closure of the Upgrade Status Ticket according to these procedures serves as certification of the site upgrade. Sites will not be required to be re-commissioned as the result of an upgrade to a new DMS product release.

#### **1114. DMS Release Testing**

The ISP provides a detailed description of the testing process for each DMS release. The process is divided into three phases:

- a. DMS Product Testing.
- b. DMS Integration Testing.
- c. DMS Verification Testing.

While DMS Product and Integration testing are critical to the deployment decision, Verification Testing is key to determining whether or not the new release has been installed successfully. The following provides a brief summary of the three phases.

##### **1114.1 DMS Product Testing**

DMS Product Testing is performed jointly by the DMS integration contractor and the JITC. The test is conducted in the DMS integration contractor integration and test lab. The focus of testing is on new builds received from the product vendors. The tests performed verify that a particular product can be correctly installed, can be configured, and that all required functions are working. The next step in the DMS product test is a system level test performed to verify interoperability of the entire suite of release products.

### 1114.2 DMS Integration Testing

DMS Integration Testing is performed by JITC over a Wide Area Network (WAN) to assess the product release performance in a WAN environment rather than a lab environment. The integration test is divided into three phases.

a. Integration Test Phase 1.

Integration Test Phase 1 will be conducted by experienced JITC testers at three sites. This testing will ensure the system is correctly configured and that experienced personnel can successfully execute the new test scenarios. These testers also have the experience to verify the interfaces to the DTH legacy system, verify correct functioning of the Network Time Protocol (NTP) and Directory System, perform load testing, and verify fault tolerant features such as alternate routing.

b. Integration Test Phase 2.

Experience has shown that ordinary users will see and use the system differently than experienced testers do and consequently, will find problems that escape the testing process, regardless of the amount of previous testing. There simply is no substitute for "real users". JITC will address this issue by having users who are not professional testers send and receive messages during Integration Test Phase 2.

c. Integration Test Phase 3.

In Integration Test Phase 3, JITC will complete their evaluation of the system. In this phase all components, including the endpoints, will be upgraded to the new release level. Experienced testers will perform this evaluation in a lab environment.

### 1114.3 DMS Verification Testing

Verification testing consists of a series of tests designed to verify that the primary DMS functions are working correctly together as a system after installation of a new product release at a site. Verification testing will be performed by each infrastructure and Navy LNOSC site after completing upgrade procedures to certify that their DMS configuration is performing properly. The test procedures are provided in the ISP. These procedures are generic and have not been tailored to any particular site. Each site should perform only the tests that apply to its particular enclave. Successful execution of the verification tests is required to close the DMS Upgrade Status Ticket and declare the site upgrade complete.

#### 1114.4 Navy Verification Testing

COMNAVCOMTELCOM may, as the situation warrants, have Navy LNOSC'S conduct additional testing to ensure that unique Navy operational requirements are met by the new product release. Should any such tests, beyond those in the ISP, be needed, COMNAVCOMTELCOM will prepare test procedures and coordinate them with the DMS GSM prior to asking the Navy LNOSC(s) to carry out the testing.

**CHAPTER 12****DMS REPORTING PROCEDURES****1201. General**

This chapter prescribes procedures for the system monitoring and reporting necessary to allow DISA, DCOC, and COMNAVCOMTELCOM to assess DMS performance and to manage the DMS accordingly.

**1202. System Monitoring**

System monitoring is a function of the SMS and provides management with tools to judge the reliability, availability, and speed of service of the DMS. Some of the information needed for long-range and contingency planning is obtained through a data collection process. Additional performance monitoring is based on information available on a real-time basis and is used by network managers to evaluate network performance and to correct trouble conditions as they occur.

**1203. Navy LNOSC Automated System Management Reporting**

System Management Reporting addresses the need to efficiently manage the system. This reporting is accomplished by regularly polling the various Management Information Base (MIB) agents that run on each component and collecting data from each MIB. This data effectively represents a variety of operations, including messages out, message conversion, and system performance. This data is used in two reports: the CumStat and the SysStat. The CumStat is representative of messaging and processing, while the SysStat shows system performance. A third report, the Summary Statistics Report, provides a summary of collected information for each RADAY on the components within a domain or area of responsibility. The following describes the method of generating these reports if they are not generated automatically at RADAY change.

**1204. Activation of the Reports**

The Reports are activated from a pull-down menu in the work space area using a left click of the mouse. This displays an HP work menu. Select the **Stat Reports** option and the menu offers the following choices:

- a. System Status Report
- b. Cumulative Statistics Report

**1205. System Status Report**

This report will be generated just before the daily counts are reset and retained for a minimum of 30 days. MLA, MWS, and DSA data will also be gathered and included in this report. The

report will be forwarded to the servicing RNOSC and, if so configured, to a Navy or USMC monitoring center. The reporting site will use the report to analyze system trends and to ensure system performance is not degraded.

The following paragraphs provide an explanation of the different parts of the System Status Report, as well as directions for activating and running the report.

### **1205.1 Requesting the System Status Report**

At the MWS, the operator uses the "HP VUE Background Menu" to activate the System Management Reports. From the "Background Menu", the operator selects the "Stat Reports" option. This provides a drop-down menu, from which the operator selects "System Status" menu.

a. The System Stat can be executed from a hpterm window by typing the command: **/users/mws/bin/SysStat\_sh**

b. The default output file is **/userd/mws/reports**; however, the output of the report can be directed to a specific file by the requester of the report.

### **1205.2 Customizing the System Status Report**

When the System Status Report is requested, a pop-up window is displayed allowing the operator to customize the report.

a. The date shown is the current date. This date can be modified, since the MWS retains 14 days of Simple Network Management Protocol (SNMP) on-line data from which a SysStat can be generated.

b. The hours for the report can be modified if needed. The default is a full 24-hour period. If the Stop hour is past the current hour, the system is forced to stop at the current time.

c. The component type can be modified for a specific component. The default is all components.

Figure 12-1 and Figure 12-2 show the System Status Report Request Window and a portion of a System Status Report.

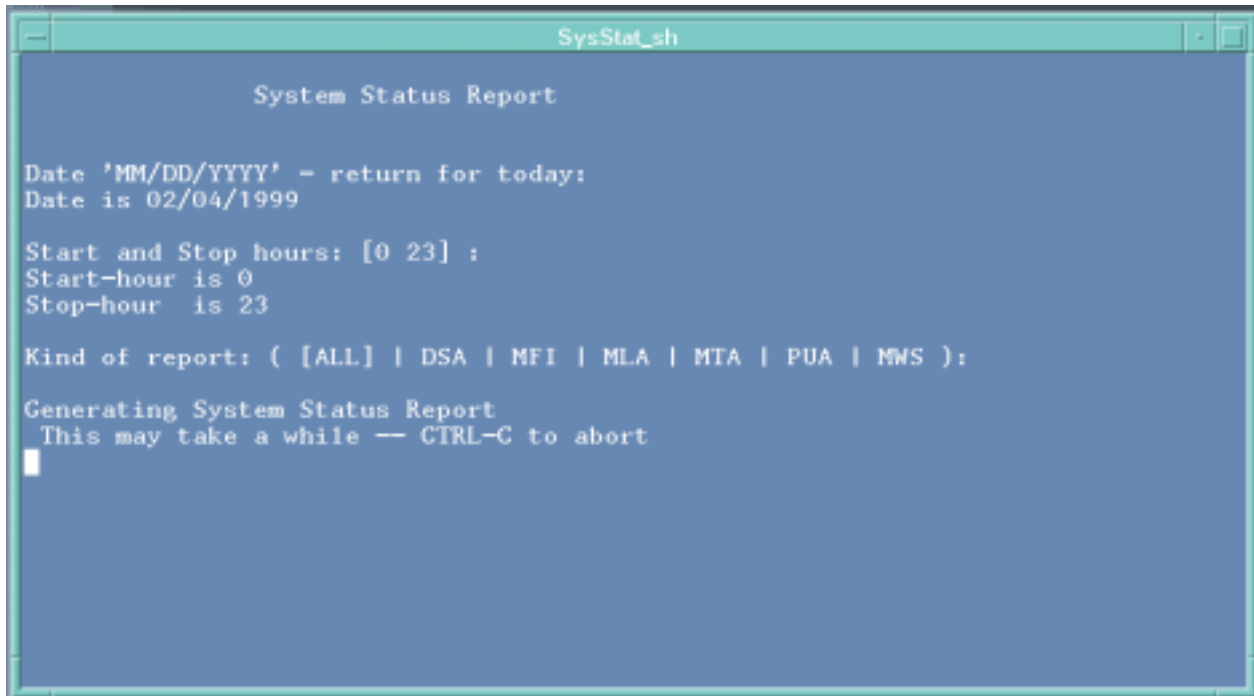


Figure 12-1

System Status Report Request Window

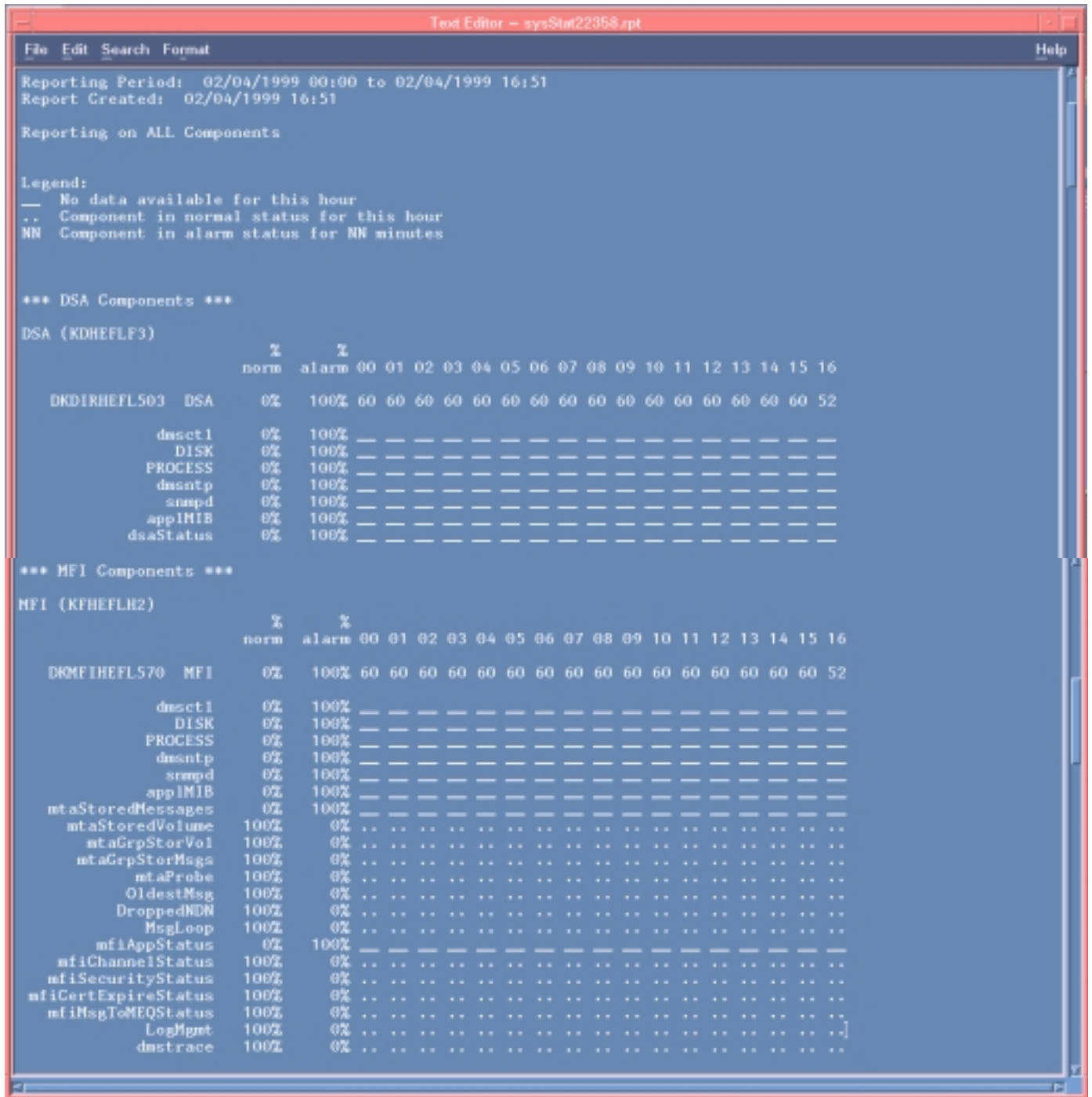


Figure 12-2

System Status Report (Partial)



## 1206. Cumulative Statistics Report (CumStat)

This report is generated upon operator request or automatically at the end of each RADAY. The report will be retained for a minimum of 30 days. All items in this report are reset at the end of each RADAY. The report will be forwarded to the servicing RNOSC and, if so configured, to a Navy or USMC monitoring center. The reporting site will use the report to review station performance totals, to analyze component trends, and to ensure that component performance is not degraded.

The following paragraphs provide an explanation of the different parts of the CumStat, as well as directions for activating and running the Report.

### 1206.1 Activating the Cumulative Statistics Report

At the MWS, the operator uses the "HP VUE Background Menu" to activate the System Management Reports. From the "Background Menu", the operator selects the "Stat Reports" option. This provides a drop-down menu, from which the operator selects "System Status" menu.

The operator uses the "HP VUE Background Menu" to activate the Cumulative Statistics Reports, selecting the "Stat Reports" option. This provides a drop-down menu. Select "Cumulative Status" from this menu.

a. The CumStat can be executed from a hpterm window by typing the command: `/users/mws/bin/CumStat_sh`

b. The default output file is `/userd/mws/reports`; however, the output of the report can be directed to a specific file by the requester of the report.

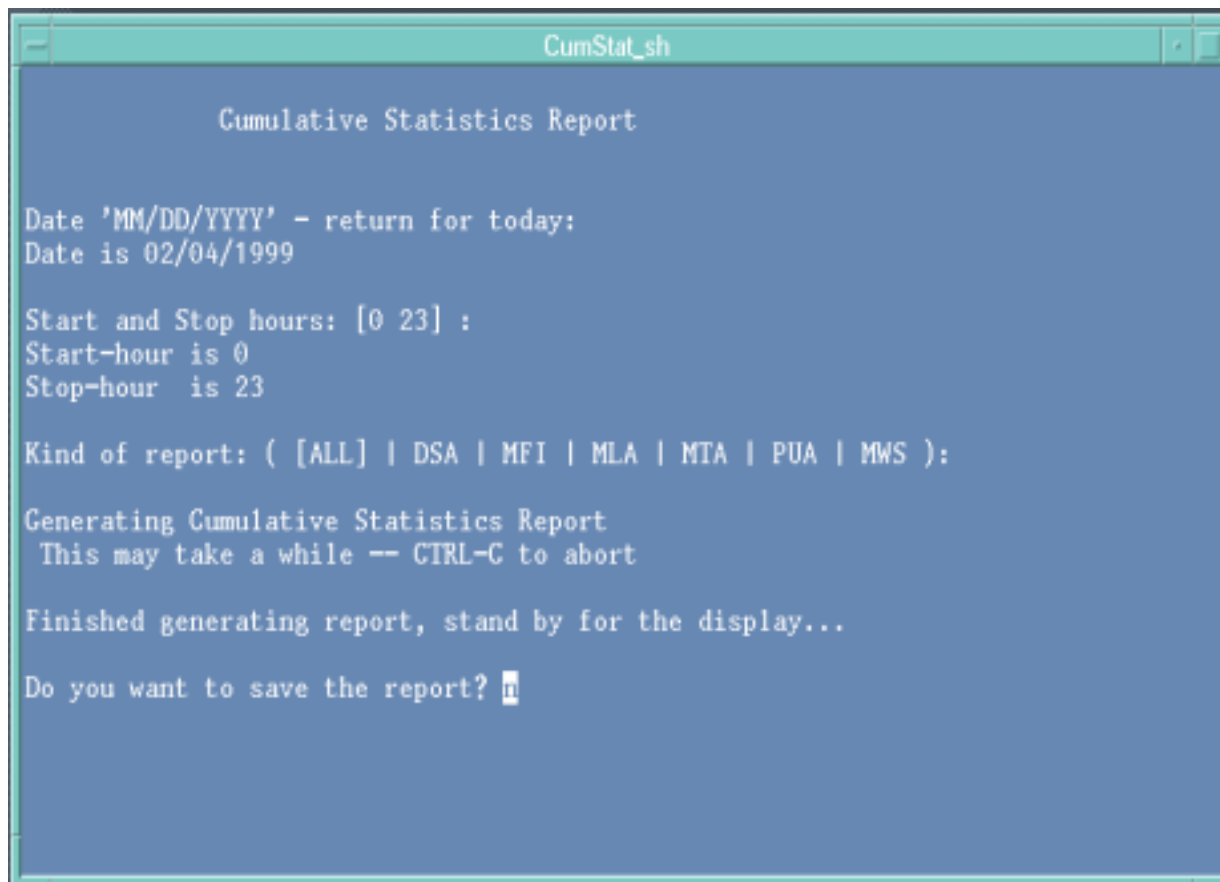
### 1206.2 Customizing the Cumulative Statistics Report

a. The date shown is the current date. This date can be modified, since the MWS retains 14 days of SNMP on-line data from which a CumStat can be generated.

b. The hours for the report can be modified if needed. The default is a full 24-hour period. If the Stop hour is past the current hour, the CumStat is forced to stop at the current time.

c. The component type can be modified for a specific component. The default is all components.

Figure 12-3 and Figure 12-4 show the Cumulative Statistics Report Request Window and a portion of the Cumulative Statistics Report.



```
CumStat_sh

Cumulative Statistics Report

Date 'MM/DD/YYYY' - return for today:
Date is 02/04/1999

Start and Stop hours: [0 23] :
Start-hour is 0
Stop-hour is 23

Kind of report: ( [ALL] | DSA | MFI | MLA | MTA | PUA | MWS ):

Generating Cumulative Statistics Report
This may take a while -- CTRL-C to abort

Finished generating report, stand by for the display...

Do you want to save the report? █
```

Figure 12-3

Cumulative Statistics Report Request Window

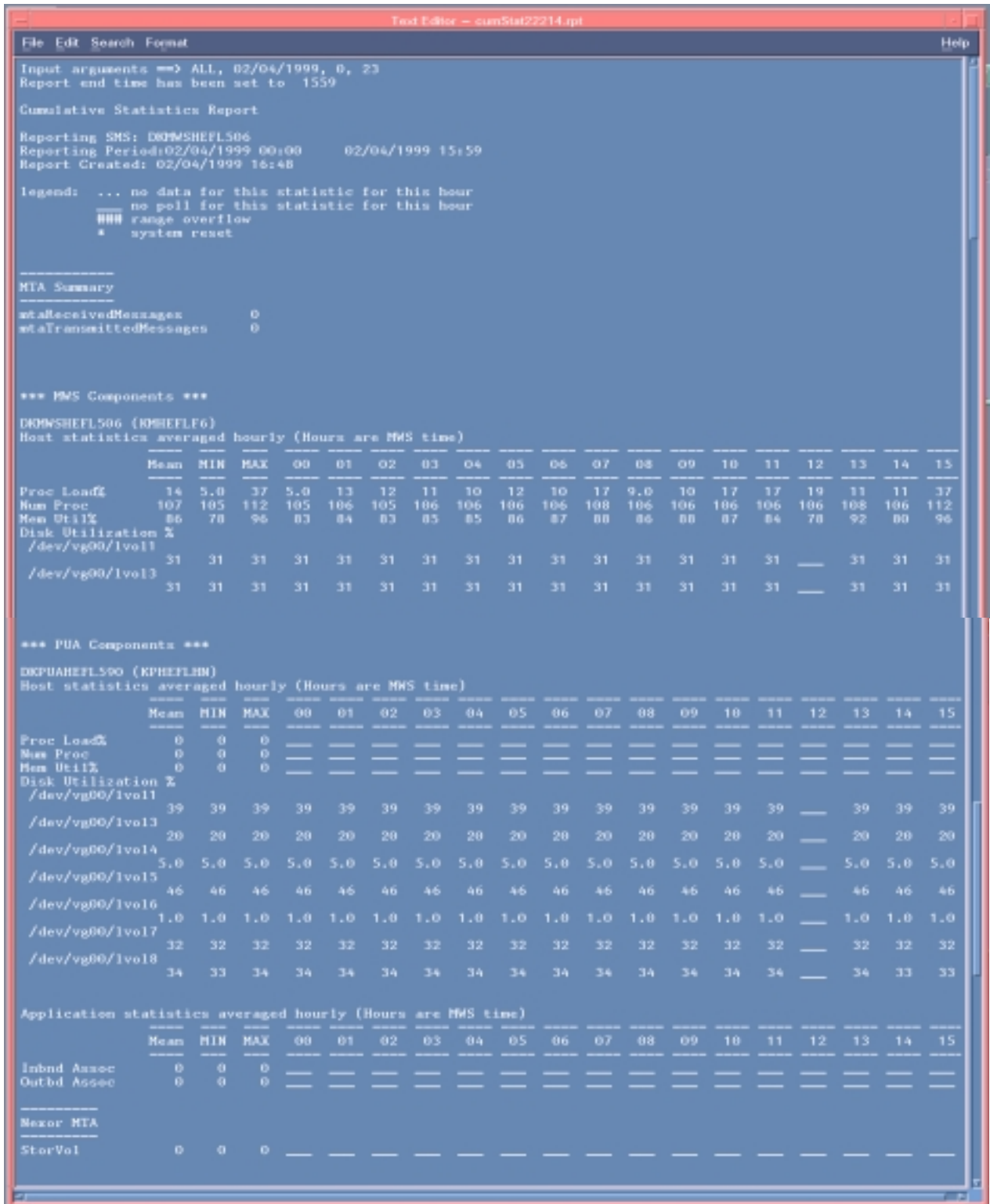


Figure 12-4

Cumulative Statistics Report (Partial)

**1207. Non-automated Reporting Requirements****1207.1 Daily Navy LNOSC Summary Report**

This report contains all significant events occurring during the previous RADAY. Sections of this report may be formatted where appropriate. Many items appearing in this report will be in narrative form. Some information may be redundant with respect to other reports previously generated during the reporting period, e.g. denial of service, possibly relating to a security incident, will have been reported immediately following detection but will also be included in this report. The report is mainly used for historical tracking and will be forwarded to the RNOSC and, if so configured, to a Navy monitoring center as required.

**1207.2 Daily Navy LNOSC System Performance Report**

This is a report of system problems not reported by a trouble ticket. The following system problems will require notification to the RNOSC or COMNAVCOMTELCOM:

- a. System and network security incidents.
- b. High precedence message delays.
- c. Excessive non-delivery notifications.
- d. Non-deliveries due to DMS component failure.
- e. Activation of new or transferred components.
- f. Planned outage for an infrastructure component.
- g. Hazardous Condition (HAZCON) for a Navy LNOSC or infrastructure component.
- h. Service activations and terminations.
- i. Trouble ticket summary, including the number of tickets opened, the number closed, and the number open more than 12 hours.

**1208. Routine or Historical Operations**

This report will be submitted by Navy LNOSC'S as directed by COMNAVCOMTELCOM. The type of information which needs to be reported across management boundaries for routine operations or historical purposes includes:

- a. High precedence message delays due to reasons associated with hardware, software, network, or operating personnel deficiencies.

b. Hazardous conditions, such as equipment or environmental problems, which could potentially result in a component failure.

c. Summary of component outages, planned or unplanned, whether or not previously reported. Planned outages will have been coordinated in advance and notifications provided accordingly. Reports of unplanned outages, whether caused by software or hardware failure, will include a summary of the analysis performed and the action taken to resolve the problem and to restore operations. This includes components in HAZCON, where redundant or "backup" equipment is installed but is not available, either because the original equipment is in an outage condition and the backup in use, or the backup is in an outage condition.

d. Statistics for each MHS infrastructure component (MTA, MFI, MLA), especially for those components, which interface with a component in the other management domain. The information for these components should also include statistics concerning the amount of system resources (Central Processing Unit (CPU), memory, disk space, swap space) in use.

e. Statistics for each DSA are necessary for day-to-day directory management and to aid software and system engineering personnel in isolating and resolving causes for directory service failures. The information for these components should also include statistics concerning the amount of system resources including CPU, memory, disk space, and swap space, in use.

f. Performance statistics for each MWS, including system availability and the periods of high activity, percentage of resources (CPU, memory, disk space, swap space) in use, and reasons for peak processing (resource consumption exceeding some threshold).

g. Trouble ticket statistics include the number of trouble tickets escalated between management centers. This information is necessary for the analysis of DMS fault management as well as being useful for the analysis of customer support requirements. Ideally, a summary of trouble tickets should be maintained on a DMS bulletin board for reference by the LCC or RNOSC operations or helpdesk personnel. Trouble tickets open against operational problems associated with software or hardware should be posted, along with suggested workarounds, until the problem can be resolved.

h. Activation or de-activation of mail lists. These are controlled and accountable.

i. Suspected data interlace occurrences not detected by either hardware or software. All information relative to such an incident would be needed to identify and isolate the failed

component. This problem should result in the generation of a trouble ticket.

j. DMS system configuration changes (notices and implementations).

k. Complete domain information for the backup MWS if one is designated. Updates or modifications to this information need to be provided to the backup MWS in a timely fashion.

#### **1209. DMS Asset and Inventory Control**

The type of information which needs to be reported across management boundaries in support of DMS asset or inventory control includes:

a. Notification of the implementation of a new software release. This information is necessary for DMS software configuration management.

b. Notification of the implementation of hardware upgrades. This information is necessary for DMS configuration management.

c. Activation of new components and associated users. This information is necessary for DMS configuration management.

d. De-activation of existing components and associated users. This information is necessary for DMS configuration management.

e. Results of periodic inventory of Fortezza cards for infrastructure components.

f. Summary of customer base information. This information is necessary for periodic performance and trend analysis, as well as DMS configuration management.

#### **1210. Report Retention**

All reports will be retained in the Navy LNOSC archives for a minimum of 30 days.

**CHAPTER 13****CONFIGURATION CHANGE PROCEDURES****1301. General**

This chapter prescribes procedures for implementing changes at commissioned Navy LNOSC'S that require reconfiguration of the DMS backbone infrastructure and update of the DMS Master System Detail Design (MSDD). The procedures apply to proposed configuration changes planned or required at commissioned Navy LNOSC'S. Of particular concern are design changes which require reconfiguration (e.g., updating the routing tables) of the DMS infrastructure by the RNOSC.

**1302. Scope**

The procedures in this chapter apply to both changes to components at commissioned Navy LNOSC sites that directly interface with the DMS backbone infrastructure and to those which do not. Figure 13-1 shows the process for making changes at Navy LNOSC sites.

a. The following components are those which interface with the backbone infrastructure:

- (1) Primary GroupWare Server (PGWS).
- (2) Backup GroupWare Server (BGWS).
- (3) Local Directory Systems Agent (LDSA).
- (4) Local Message Transfer Agent (LMTA).
- (5) Mail List Agent (MLA).
- (6) Profiling User Agent (PUA).

b. CHAPTER 2 and CHAPTER 3 describe these components and their interface with the DMS backbone infrastructure. The procedures in this chapter are applicable to the following detailed design changes:

- (1) Component addition or removal.
- (2) Component name change.
- (3) Component host name change.
- (4) Domain name change.
- (5) DIT Level 6 change.

b. Procedures for updating the MSDD for changes that do not directly affect the backbone infrastructure are also provided.

**1303. Design Validation Team (DVT)**

a. The DVT is the DISA office responsible for maintaining the MSDD. The MSDD is a collection of all DMS site detailed designs and reflects the current configuration of the global DMS. The DVT is responsible for ensuring that site configuration

changes are compatible with the overall architecture by validating changes submitted by the Services and Agencies.

b. The DVT is the interface between the RNOSC and the Navy regarding changes at Navy LNOSC. The Navy shall identify to the DVT the design representatives authorized to submit design changes to the DVT (herein referred to as the Navy POC). The Navy POC shall be a qualified DMS engineer, capable of preparing and updating DMS Detailed Designs. Normally, the Navy POC will be from the Navy DMS engineering activity. The DVT will only accept Navy LNOSC site changes from the designated Navy POC; the RNOSC will only execute changes validated by the DVT. The DVT contact information is as follows:

Address:

Lockheed Martin Federal Systems  
Mail Stop 120-025  
Attn: DISA DMS Design Validation Team  
9500 Godwin Drive  
Manassas, VA 20110-4157

Phone:

Commercial (703)367-6692  
Fax (703)367-3723

DMS Account: A DMS Organizational account is currently being established for the DVT and will be included in this procedure prior to initial distribution to the field.

#### **1304. Design Review Order and Precedence**

Navy LNOSC site design changes received by the DVT will be reviewed in the order they are received and will not be reviewed ahead of designs (new or updates) previously received by the DVT. Only the Navy POC can authorize a swap of an updated design with another design from the Navy that is already in the DVT for review. The normal timeframe for the DVT to review a design is approximately five working days. For situations that have an immediate operational impact on the site, the Navy POC may request the GSM to re-prioritize design reviews currently being processed by the DVT. The request will be transmitted via DMS signed organizational message. The GSM X.500 DN is:

C=US/O=US GOVERNMENT/OU=DOD/OU=DISA/OU=ORGANIZATIONS  
/OU=ORG STAFF/OU=OPS/CN=DMS GSM

If the GSM approves an upgrade in priority, the GSM will notify the DVT to review the design ahead of the other designs requested by the Navy POC. The DVT will modify the priority for design reviews when directed by the GSM. The GSM will also notify the RNOSC to provide priority support as required to the site, to include providing infrastructure testing ahead of other sites awaiting testing. Immediate design reviews will be



accomplished by the DVT within 24 hours of receipt of the updated design.

### **1305. Detailed Designs**

Prior to the initial installation, acceptance, and commissioning, a detailed design is produced and validated for each site. This design is integrated into the MSDD. Following commissioning, changes to Navy LNOSC sites will be documented by updating the Navy LNOSC site detailed design. The detailed design provides all the data required for configuring DMS components. A copy of the validated detailed design is provided to the site and to the Navy DMS Program Management Office (Navy PMO) by the DVT. The DVT and the RNOSC also maintain a copy of each Navy LNOSC detailed design.

a. The Navy is responsible for updating the detailed design when a change is made to a commissioned Navy LNOSC. Changes will be made to the detailed design using the Detailed Design Tool (DDT).

b. The DDT is a software application that was developed to automate the preparation and update of DMS detailed designs and to simultaneously populate and update the MSDD database. Only the Service or Agency POC'S identified to the DVT can receive and use the DDT. The DVT will provide instructions for DDT registration when the Services and Agencies identify their design POC'S.

c. The DDT user manual provides instructions for using the tool and how to submit updates to the DVT. The tool and the manual are available through a File Transfer Protocol (FTP) server. The address and procedures for accessing the FTP server are available from the DVT.

### **1306. Changes Involving the Backbone Infrastructure**

The following change procedures apply to Navy LNOSC changes requiring reconfiguration of the backbone infrastructure. Paragraph 1306.1 describes routine change procedures and Paragraph 1306.2 addresses emergency change procedures.

#### **1306.1 Routine Change Procedures**

The Navy POC will send an updated Navy LNOSC site detailed design to the DVT for validation before initiating implementation of the change at the site. Changes will be submitted using the DDT according to the procedures in the DDT manual. The Navy POC will identify the changes that were made in the DDT Change Control Form. Without the changes identified explicitly in the Change Control Form, the DVT can not determine what changes were made. As a result, corresponding RNOSC infrastructure changes will not be made and the site's messaging capability could be impaired.

(1) The DVT will review the proposed change to ensure it is compatible with the DMS infrastructure. The Navy can expect the design review to be completed within one week from the date the DVT receives the design or within 24 hours if the GSM has directed an immediate response. If the change is acceptable, the DVT will validate it and update the MSDD accordingly. The DVT will send the validated site detailed design to the servicing RNOSC and notify the Navy POC that the design has been validated. If the site design was directed by the GSM to be reviewed ahead of other sites, the DVT will advise the RNOSC accordingly. The site must coordinate with its servicing RNOSC prior to initiating implementation of the validated change(s). If there are issues or concerns with the proposed new design, the DVT will contact the Navy POC and provide a listing of the specific items of concern. The DVT will then await a Navy response (by signed DMS Organizational message, fax or mail) before re-evaluating the design change. The Navy POC is responsible for coordinating a response within the Navy and providing this response to the DVT.

(2) After the DVT has validated the change, the servicing RNOSC will notify COMNAVCOMTELCOM that the change is ready, and COMNAVCOMTELCOM will direct the Navy LNOSC to implement the change and establish a test schedule. The Navy LNOSC will submit a trouble ticket to its servicing RNOSC before implementing the change. The ticket will identify the projected schedule for implementing the change including the date the LNOSC expects to be ready for testing with the RNOSC. This will alert the RNOSC that the change is being implemented and that the RNOSC should reconfigure the backbone infrastructure according to the validated design.

(3) The Navy LNOSC will complete local testing of the change prior to testing with the backbone infrastructure. When local testing is complete, the Navy LNOSC will advise the RNOSC through the Navy management chain that infrastructure testing may be initiated.

(4) The RNOSC will provide the infrastructure testing schedule to COMNAVCOMTELCOM, who will pass it to the Navy LNOSC. The RNOSC will schedule infrastructure testing in the order that requests are received from the Navy LNOSC'S. The timeframe between when the ACC contacts the RNOSC and when actual testing begins depends on the number of sites waiting to be tested and other operational circumstances. Sites will not be tested ahead of sites already in line to be tested. Only the Navy POC can authorize a site to be tested ahead of another site from the same service. The RNOSC will only provide infrastructure testing out of order when directed to by the GSM. When infrastructure testing is successful, the RNOSC will annotate the trouble ticket and close it.

(5) If backbone testing of the validated detailed design results in a change to the new design, the Navy POC will identify

the required change (via a signed DMS organizational message) to COMNAVCOMTELCOM, the RNOSC, and DVT before the RNOSC or Navy LNOSC is authorized to implement the change. The DVT will update the MSDD and forward the updated copy to COMNAVCOMTELCOM, the RNOSC, the Navy LNOSC, and the Navy POC.

#### **1306.2 Emergency Change Procedures**

An emergency situation is an unforeseen condition that results in the immediate loss of DMS organizational messaging capability to all or a portion of the organizational messaging users supported by the site. If this condition requires an infrastructure level change in order to restore organizational messaging service, the design validation process can be postponed. Instead, the change will be coordinated between the Navy POC and, if necessary, the Navy LNOSC and the RNOSC. The RNOSC will respond immediately to reconfigure the backbone infrastructure as required by the changes made to the local site components. Afterwards, the Navy will update the local site detailed design and send it to the DVT within 48 hours after the change is implemented. The DVT will review and validate the design according to the procedures in Paragraph 1306.1 above.

#### **1307. Changes Not Involving the Backbone Infrastructure**

These procedures apply to other local changes that do not involve components connected to the backbone infrastructure. These procedures are required to ensure that the MSDD is up to date for operational and engineering reference to use for troubleshooting and system configuration management. When a change is implemented at a Navy LNOSC, the Navy is responsible to update the Navy LNOSC detailed design using the DDT. The Navy POC will send the updated detailed design to the DVT. The DVT will update the MSDD and provide it to the RNOSC.

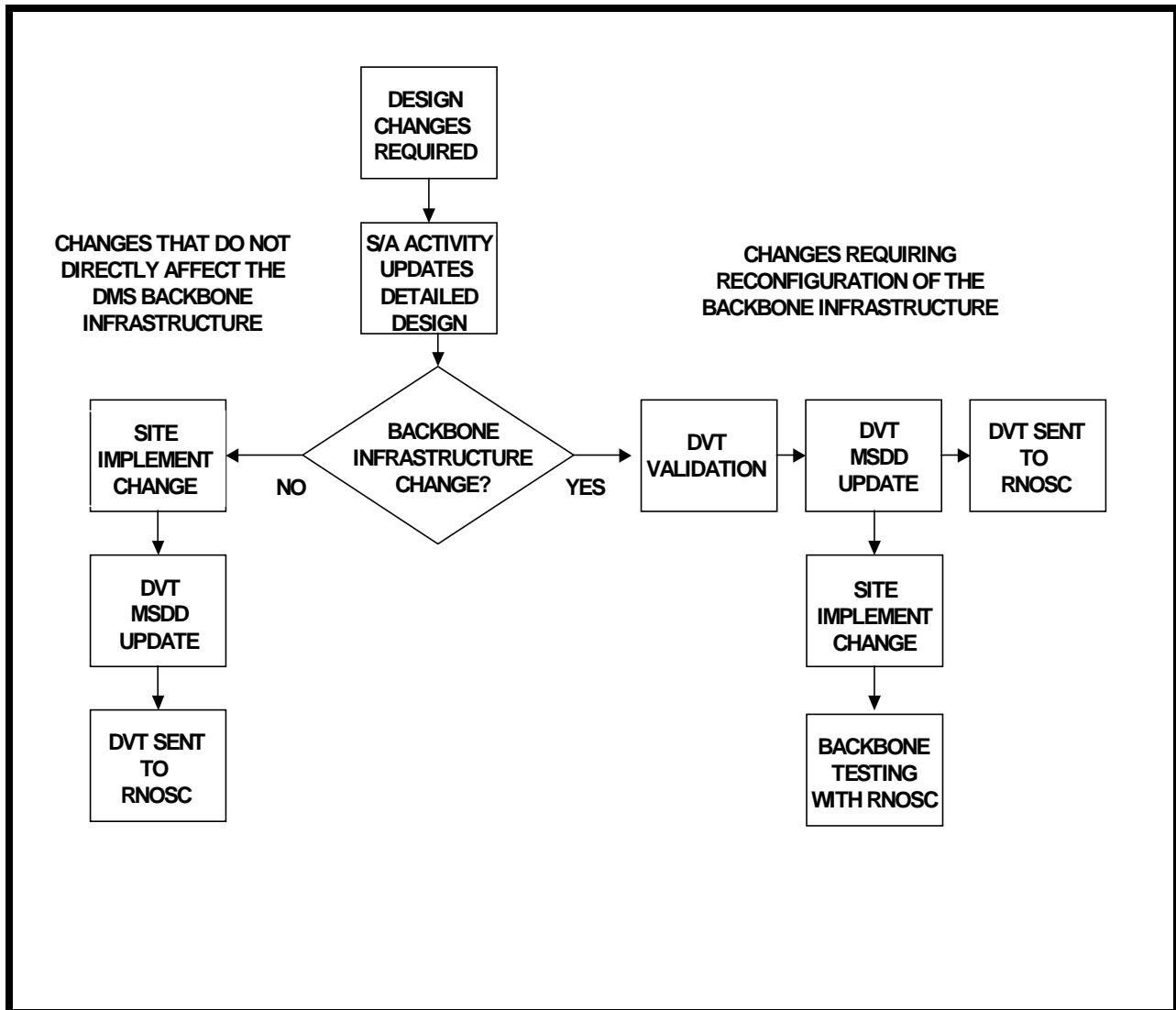


Figure 13-1

Detailed Design Change Process

CHAPTER 14HIGH ASSURANCE GUARD PROCEDURES**1401. General**

This chapter describes the HAG'S, their placement and purpose, and procedures for their use and maintenance.

The NSA-approved HAG will be used to support communications between DMS security domains. The HAG is configurable to allow or disallow X.400 and X.500 communications based on filters within the HAG. By DISA policy, the HAG will only support communications between adjacent security domains, that is between Unclassified and Secret and between Secret and Top Secret. The current use of the HAG is to support both high-to-low and low-to-high exchange of Unclassified message traffic between the Secret and Unclassified domains, and to support shadowing of Directory information from Unclassified to Secret DSA'S. In order to simplify the configuration of routing information, each DMS domain will be a separate Private Management Domain (PRMD) within the existing DMS Administrative Management Domain (ADMD).

The ADMD value for DMS is "DMS"; the PRMD value is "dms+gov+SIPR" for the Secret domain. The Unclassified domain typically does not have a PRMD value. The physical placement of the HAG is at a local site which hosts a Secret enclave. A few HAG'S will be placed within the backbone to provide Directory shadowing for the upper levels of the DMS Directory. For those organizations which have no HAG in their environment, a Memorandum of Understanding (MOU) may be entered into with another organization to use that organization's HAG.

**1402. HAG Placement**

The HAG is physically placed within the higher level enclave. Messages between users within the same domain do not need to go through the HAG. In the Secret domain, however, a message originator must use the originator personality appropriate to the message classification and must also address the appropriate personality of the recipient(s). When a user in the Secret domain, using the unclassified personality, addresses an unclassified message to recipient(s) in the unclassified domain, the User Agent must automatically include a token for the HAG so that the HAG can decrypt the message and verify that it is allowed to pass to the unclassified domain. PUA'S and MLA'S must also include a HAG token when addressing messages to recipients in the unclassified domain.

Non-Delivery Notifications and Delivery Reports will be allowed to pass the HAG in either direction, since they are automatically generated and cannot contain classified data. Alternate delivery service is allowed through the HAG only when

both the original recipient and the alternate recipient are in the same domain.

A user in the secret domain need not address a message specifically to a particular HAG. The determination of the appropriate HAG is made based on the recipient's address and the configured routing information.

#### **1403. HAG Keyword Criteria**

The HAG has the capability of searching for message classification and specified keywords. Local requirements will determine the classified keywords in use in the higher domain and which the HAG must prevent being passed to the lower domain. More information will be provided as it becomes available.

**CHAPTER 15****FIREWALL PROCEDURES****1501. General**

This chapter identifies the operational impact of DoN-implemented network firewalls on DMS protocols and provides the operational policy and procedures between the RNOSC and Navy LNOSC'S when firewalls limit full use of those protocols.

A firewall is a type of access control gateway, which is placed between a private or restricted access network and a public network to selectively filter incoming and outgoing traffic by protocol. In DMS, a firewall is placed at the infrastructure level and is designed to allow passage of only certain protocols. For example, a firewall may allow passage of DMS messaging protocol, but not directory access protocol. Unlike the HAG, a firewall does not scan the header or contents of a message.

**1502. Firewall Description**

A firewall is used to establish a protected environment and encompasses all components within a protected enclave such as an agency's site. The DMS Firewall Configuration Guidance document provides in-depth technical explanations and analysis of firewalls and their impact on the DMS. This document is available in the DMS Online Library. The DMS Online Library is accessible through the DMS Controlled Access Web Page. A link to this Web page is provided through the NAVCOMTELCOM Web site at "[www.nctc.navy.mil](http://www.nctc.navy.mil)".

**1503. Local Firewall Implementation**

Services and Agencies implement firewalls in accordance with their own network security policy. However, when those firewalls are located between the local DMS enclave and the DMS backbone infrastructure, DMS operation and systems management can be affected. Sites will differ, but Figure 15-1 illustrates a common local network security policy implementation of a firewall and shows the effect on DMS operations.

**1504. Policy**

Navy LNOSC ASM'S and LSM'S will work with local network and firewall administrators to ensure that firewalls are configured to allow passing of X.400 and X.500 protocols for DMS organizational messaging and directory services. ASM'S and LSM'S are expected to remain cognizant of the configuration of their local network firewall and the impact on DMS operation and management between the local site, the DMS backbone infrastructure, and the servicing RNOSC.

### 1505. Protocols

Table 15-1 identifies the protocols and associated port utilized by DMS for messaging, directory services, system management, and system control. It identifies the affected local components, affected regional components at the regional nodes and RNOSC'S, and the function the protocol facilitates. The shaded rows indicate the protocols commonly blocked by local firewalls due to security concerns and policy. However, it is possible for other protocols to be blocked depending on the site's individual network security policy and firewall implementation.

### 1506. Protocol Guidance

Procedures for each of the identified protocols blocked by a local firewall are as follows:

- a. X.400, P1 Protocol.

This protocol will not be blocked by local firewalls.

- b. X.500 Directory System Protocol (DSP), Directory Information Shadowing Protocol (DISP), and Directory Access Protocol (DAP).

These protocols will not be blocked by local firewalls.

- c. FTP Incoming.

When the FTP protocol is blocked from entering (e.g. RNOSC MWS to Navy LNOSC MWS) the protected enclave, the servicing RNOSC will not be able to retrieve log files from site components and subsequently be unable to perform a message trace to the site. In this situation, the RNOSC will trace to the last BMTA on the message route and then pass a request for message trace continuation to the Navy LNOSC. The procedures in CHAPTER 9 apply.

- d. FTP Outgoing.

Normally, outgoing FTP (e.g. Navy LNOSC MWS to RNOSC MWS) is not blocked; however, when it is blocked, the site will be incapable of transferring trouble tickets and messaging reports to the RNOSC. In this event, trouble tickets will be forwarded via DMS operations messages. The message will contain all the information normally provided in a trouble ticket.

- e. SNMP (Trap).

SNMP (Trap) is used for local component monitoring only and does not affect interoperability between the Navy LNOSC and the RNOSC.



## f. SNMP (Get/Set).

The SNMP (Get/Set) protocol is used by the RNOSC to monitor and control local components listed in Table 15-1. When this protocol is blocked, the RNOSC will not be able to determine the status of local components if a problem occurs. In this situation, the Navy LNOSC ASM or LSM is responsible for notifying the RNOSC by operations message whenever one of the listed components is out-of-service.

## g. Network Time Protocol (NTP).

NTP is normally used to establish time synchronization with an external component. When NTP is blocked by a local firewall, time may be obtained from a local component or filtered through the firewall to an external server. This is a local decision.

## h. Telnet.

Telnet sessions between the RNOSC and Navy LNOSC components require strong authentication. This protocol is only used when FTP is not available through the MWS or other contingency situation. The RNOSC and ACC or LCC will coordinate the use of Telnet when it is required.

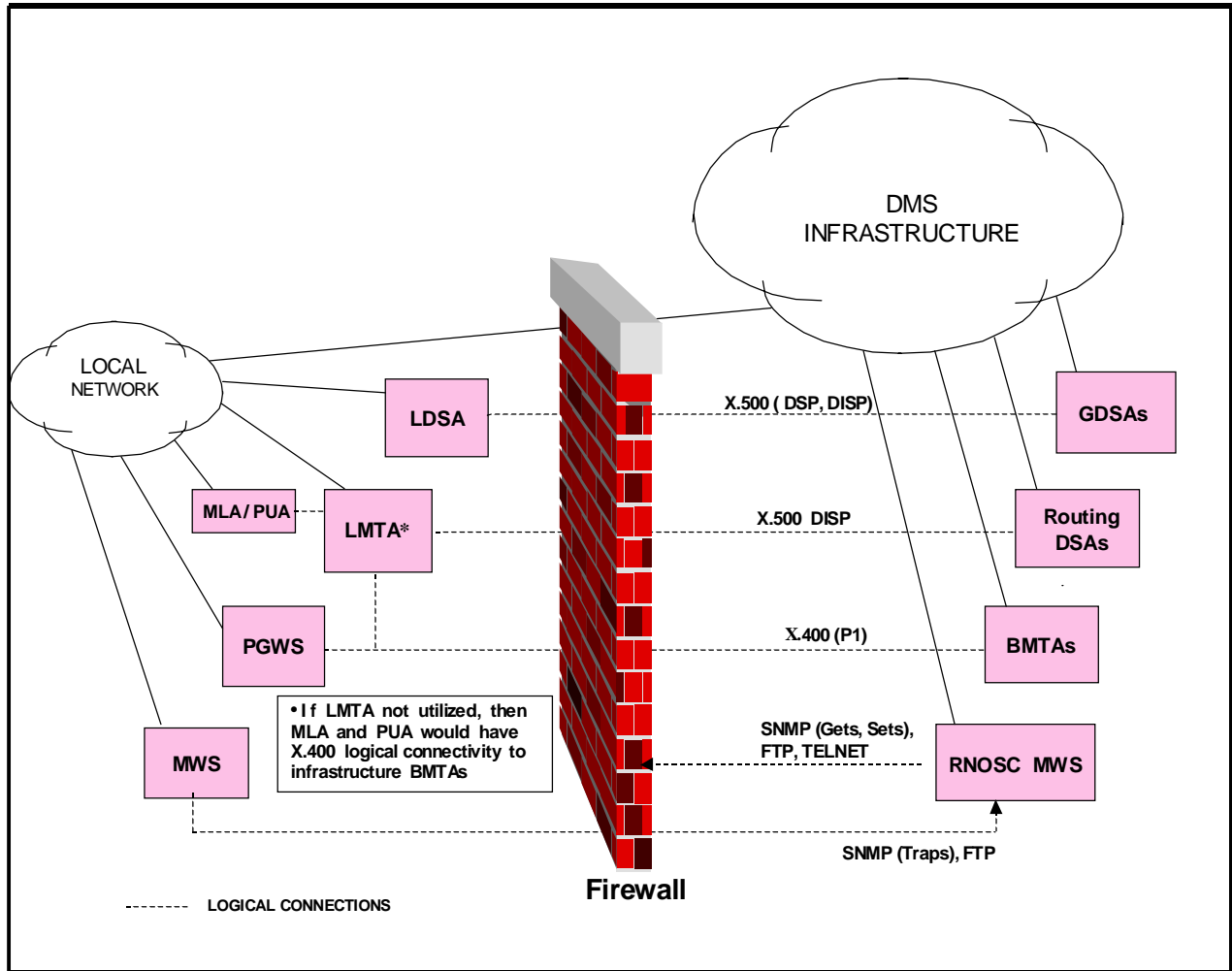


Figure 15-1

Common Local Network Firewall Implementation

PROTOCOL	LOCAL COMPONENT	REGIONAL COMPONENT	FUNCTION
X.400 P1 Port 102	PGWS LMTA MLA PUA	BMTA	Message Transfer
X.500 DSP DISP Port 17003	LDSA	RGDSA MGDSA SGDSA Master PLA DSA Shadow PLA DSA	Chaining Shadowing
X.500 DISP Port 104	LMTA	Domain (Shadow) Server/Routing DSA	RCDB Shadowing
X.500 DAP Port 104	LMTA	RNOSC-ADUA	Admin
FTP Locally Initiated Port 20 (Data) Port 21 (Control)	MWS	RNOSC-MWS	-Trouble Ticket Transfer -Messaging Reports -MWS Back-up Map/Hosts
FTP RNOSC Initiated Port 20 (Data) Port 21 (Control)	PGWS LMTA MLA PUA	RNOSC-MWS	Log Retrieval/ Message Trace
SNMP (Trap) Port 162	MWS PGWS LMTA MLA PUA	RNOSC-MWS	Monitor
SNMP (Get/Set) Port 161 (Native HP-UX) Port 26017 (Agent) Port 6664/5 (Agt Factory)	MWS PGWS LMTA MLA PUA	RNOSC-MWS	Monitor and Control
NTP Port 123	PGWS LMTA MLA PUA LDSA MWS ADUA	BMTA SGDSA	Time Synchronization
Telnet Port 23	MWS	RNOSC-MWS	Configuration Control

Note: The shaded rows indicate the protocols commonly blocked by local firewalls due to security concerns and policies.

**Table 15-1**  
**Firewall Protocol**

**CHAPTER 16****SERVICE INTERRUPTION PROCEDURES****1601. General**

This chapter prescribes the policies and procedures for planning, coordinating, and requesting approval for DMS Authorized Service Interruptions, commonly called "Planned Outages", and to prescribe the actions to be taken in the event of Unauthorized Service Interruptions or "Unplanned Outages".

All DMS elements share responsibility for ensuring reliable messaging service to users of the DMS, and all elements, including the user, should keep service interruptions to a minimum. When authorized interruptions of infrastructure services are necessary, the interruption should be planned to minimize inconvenience to users. Users also should recognize that interruption of service at their User Agents can also result in delay of response and inconvenience to message originators. For these reasons, users must obtain concurrence in planned outages from the Navy LNOSC. The Navy LNOSC must obtain approval of planned outages of the entire Navy LNOSC or its components from the RNOSC. A Navy LNOSC request for approval of a planned outage will be submitted to the RNOSC by an Authorized Service Interruption Request Ticket through the MWS. All other correspondence regarding authorized service interruptions must be by signed and encrypted organization message.

**1602. Part-time and Dial-in Users**

Part-time service is necessary when a user does not wish to maintain a full-time messaging operation. Part-time service is scheduled, and normal service interruption during off-hour periods is not considered a service interruption. Dial-in users sign on at irregular intervals to receive or send messages. During times when they are not signed on, their UA is not available to the DMS. As with part-time service, this is not considered a service interruption as described in this chapter. In both cases, users accept the responsibility for delay in receipt of messages addressed to them.

**1603. Service Interruptions****1603.1 Authorized Outage**

An authorized or planned outage is a disruption of DMS services due to planned events which require a DMS component or facility to be removed from service for a period of 10 minutes or more. Examples would be a planned power interruption or a planned system upgrade. In the following paragraphs, it is

assumed that the service interruption will be of at least 10 minutes.

### **1603.2 Unauthorized Outage**

An unauthorized or unplanned outage is a disruption of DMS service due to such events as failure of components, an unexpected power failure, or a software failure. An unplanned service interruption will be made the subject of a trouble ticket, but additional action by the Navy LNOSC is discussed below. An unplanned service disruption traceable to an adverse security event must be handled as a System Security Incident in accordance with NAVSO P-5239-19, Computer Incident Response Guidebook.

### **1604. Outage Reporting**

All service interruptions, authorized or unauthorized (scheduled or unscheduled), must be reported in accordance with the procedures outlined in CHAPTER 11 and later in this chapter.

### **1605. Planned Service Interruption at the Navy LNOSC**

A Navy LNOSC planning a routine service interruption of the entire Navy LNOSC or of a critical component must transmit an Authorized Service Interruption Request Ticket (Figure 16-1) to the RNOSC at least 14 days prior to the start of the service interruption. Where a planned outage involves only components, which have redundant components to serve as backup, there is no need to request approval for a planned outage, but the lack of a backup creates a HAZCON which must be reported in accordance with CHAPTER 11.

A service interruption request by the Navy LNOSC shall include as an addressee the Mail List composed of the served user organizations. The request message shall be addressed to the RNOSC and copied to all users in the Navy LNOSC AOR. The request message contains the:

- a. Purpose of the scheduled interruption.
- b. Proposed date, time, and duration of the scheduled interruption, and an alternate date and time.
- c. Estimated time to restore service in the event of an emergency.
- d. Known impact on DMS service. This should include the major organizations affected and whether alternate service is required.

e. Statement of the impact if the request is not approved.

f. Primary and alternate points of contact with means of communication, e.g., telephone numbers, to be used in the event of an emergency requiring early service restoration.

#### **1606. Planned Service Interruption at the User Location**

Authorized service interruption will normally be scheduled to minimize disruption of messaging services to the organization. When the outage will be long term, or where major organizations are affected, the user should request that the Navy LNOSC provide alternate routes or alternate DMS access methods during the interruption. Plans must include restoration of operations at the earliest possible time. An organizational user planning a service interruption and requiring alternate service must notify the serving Navy LNOSC at least 7 days in advance of the start time of the interruption. If no alternate service is required, the notification message must be transmitted at least 24 hours prior to the start of the planned outage.

A notification of an authorized service interruption by a user will be addressed to the Navy LNOSC and any other users who will be involved, such as recipients of alternate routed messages. The information shall be the same as in Paragraph 1606.

#### **1607. Response to Authorized Interruption Request**

The supporting ASM or LSM (for a user) or the RSM (for a Navy LNOSC or USMC site) will evaluate the impact of the service interruption on the DMS AOR, consider contingency requirements, exercises, and other scheduled service interruptions, and will reply within four hours of receipt of the request with either:

a. Preliminary concurrence in the authorized service interruption request, or

b. A request to reschedule the service interruption, with the reason for the request to reschedule.

#### **1608. Preliminary and Final Concurrence Actions**

After preliminary approval by the RSM for a Navy LNOSC authorized outage, or concurrence by the ASM or LSM in a user outage, the RSM, ASM, or LSM will transmit an organization message to all affected organizations. If only a single user organization will be affected, other users need not be notified. If the outage will be for a Navy LNOSC, all served users must be notified and must concur with the interruption by organization message. Once concurrence is received, the Navy LNOSC will notify the RNOSC and request final approval. This request must

be transmitted at least 30 minutes before the start of the scheduled service interruption; final approval must be received before the interruption can begin.

**1609. Alternate Route Requirement**

When a Navy LNOSC service interruption will affect high priority users, the Navy LNOSC may be required to arrange for alternate route capability. This arrangement may involve a temporary connection to another Navy LNOSC and may require changes to the backbone routing configuration. Alternate routing must be coordinated with the RNOSC. A requirement for alternate routing must be included in the authorized service interruption request to the RNOSC.

**1610. Planned Service Interruption at the RNOSC**

When an RNOSC itself will be subject to a service interruption, the RSM will make the ACC'S, LCC'S, and Navy LNOSC'S in its AOR copy addressees on its correspondence with the GSM. This will allow a Navy LNOSC to advise the RNOSC of any circumstances that would make RNOSC outage inadvisable, such as Navy exercises in the AOR. The RSM and GSM will take this information into account in determining whether the service interruption should proceed.

Authorized Service Interruption Request Ticket		
Field	Entry	
Site	Navy LNOSC Requesting Service Interruption	
POC LAST NAME	Last name of Navy LNOSC primary contact for the Authorized Service Interruption	
POC FIRST NAME	First name and/or rank of primary contact	
POC PHONE	Commercial and/or DSN phone number of individual with knowledge of the Authorized Service Interruption. Include country code if applicable.	
POC E-MAIL	E-Mail address of primary contact	
SHORT DESCRIPTION	Authorized Service Interruption Request	
PROBLEM DESCRIPTION	Brief explanation of the purpose of the service interruption, components affected, proposed and alternated dates.	
USER IMPACT	Services to be interrupted; high priority organizations affected	
REMEDY PRIORITY	Priority 3	Routine: Initial request for an Authorized Service interruption will be prioritized as routine.
Diary		
<p>The following minimum essential information shall be included in the diary:</p> <ul style="list-style-type: none"> <li>• Purpose of the service interruption.</li> <li>• Proposed date, time and duration of the interruption and an alternate date and time.</li> <li>• Estimated time to restore service in the event of an emergency.</li> <li>• Known or anticipated impact on DMS service.</li> <li>• Statement of the impact if the request for service interruption is not approved.</li> <li>• Request for RNOSC support of alternate routes as required.</li> </ul>		
COMPONENT TYPE	Primary affected component(s) e.g., PGWS, LDSA.	

**Figure 16-1****Authorized Service Interruption Request Ticket**



## **1611. Emergency Service Interruptions**

In some cases, it may not be possible to schedule a service interruption as far ahead as required above. For example, an electric power provider may give only a few hours warning of an power outage. In such cases, the user must submit an emergency service interruption request. The following procedures apply.

### **1611.1 Planned Outage at the User Location**

The user must notify the Navy LNOSC by message at least one hour ahead of the outage, providing all the information listed in Paragraph 1606 and, in addition, provide the reason for the emergency service interruption request and explain why it was not possible to provide the normal notice. The user may request alternate routing service, but this service cannot be assured on short notice. Since the request would not be submitted as an emergency request if it could be rescheduled, a reschedule time need not be provided. The Navy LNOSC cannot deny an emergency outage request.

### **1611.2 Planned Outage at the Navy LNOSC**

The Navy LNOSC must submit an Authorized Service Interruption Request Ticket to the RNOSC at least one hour prior to the service interruption and follow up with a telephone call to ensure that the RNOSC has reviewed the ticket. The ticket must explain why it was not possible to provide the normal notice. The LSM may request alternate routing service, but this service cannot be assured on short notice. Since the request would not be submitted as an emergency request if it could be rescheduled, a reschedule time need not be provided. The LSM must notify all users in advance of the service interruption.

Any service interruption that does not allow one hour advance notice will be considered an unauthorized or unplanned service interruption, even if some advance warning was given.

## **1612. Trouble Ticket Reporting by the Navy LNOSC**

Immediately before a Navy LNOSC enters a period of authorized service interruption, the LSM will send a trouble ticket to the RNOSC stating that service is on the verge of interruption.

## **1613. Unplanned Outage**

Unplanned outages may occur at any time or for any reason. Common causes are failure of equipment without backup, failure of software, unexpected power outages or fluctuations, operator error, or inadvertent disconnection of equipment. When the unplanned outage is of such a nature that service cannot be restored within ten minutes, the system administrator or the system manager whose AOR includes the failed device must notify

organizations affected by the service interruption. If the failure appears to be due to a software problem, the LSM must submit a trouble ticket to the RNOSC, regardless of the duration of the outage or the extent of service interruption.

#### **1613.1 Navy LNOSC Unplanned Outage**

If an unplanned outage occurs at the Navy LNOSC due to failure of a component which has no back-up and the loss of which will affect DMS messaging, directory access, or system management, the ASM or LSM will:

a. Take action to correct any dangerous condition (e.g., an electrical short circuit), that may have been involved in the outage.

b. Take action to begin service restoration. Notify the maintenance organization responsible for the failed equipment, or begin other action to restore service.

c. Notify the RNOSC if service cannot be restored in ten minutes, if possible by trouble ticket, otherwise by telephone, commercial electronic mail, or other means.

d. Affected user organizations should then be notified by an organization message to their organizational system administrators (SA'S). If this is not possible, the SA'S can also be notified by other means. Since a Navy LNOSC may be responsible for providing service to a large number of users, calling each one may be impractical. It is recommended that the ASM or LSM cooperate with the users to establish a telephone "calling tree" for such contingencies.

e. Keep the RNOSC advised of the status as time permits and cooperate in preparation of alternate routes as required.

#### **1613.2 User Unplanned Outage**

If an unplanned outage occurs at the organizational user level, the LSM will:

a. Monitor the organizational message account to learn the nature of the problem. If no report is received in a reasonable amount of time, the LSM should contact the organizational SA and request that a report be submitted as soon as reasonably possible.

b. Monitor the status of the outage and cooperate with the user SA in any alternate route action.

c. Assist in obtaining any maintenance help as necessary.

**1614. Restoration of Service****1614.1 Restoration of Service to a User**

Following the restoration of equipment to the normal operational condition, the user will so notify the Navy LNOSC by message. The Navy LNOSC will then terminate any alternate routing and allow normal resumption of message traffic. If infrastructure alternate routing was required, the alternate may continue to receive alternate routed messages until normal delivery is fully restored. The outage is considered to begin at the time the equipment went out of service and end when service was restored, but does not include any time required to remove alternate routing.

**1614.2 Restoration of Service of a Navy LNOSC**

Following restoration of equipment to the normal operational condition, the LSM will clear the outage trouble ticket with the notation that the service interruption has been terminated and that normal service has been restored. The Navy LNOSC and RNOSC will remove any alternate routes and restore normal traffic flow. The LSM must notify users by message that normal Navy LNOSC operations have been resumed.

**CHAPTER 17****NAVY LNOSC AND USMC/USCG LCC BACKUP PROCEDURES****1701. General**

This chapter provides procedures for the backup of the component systems at the Navy LNOSC.

**1702. Component System Backup Procedures**

The system backup of a component copies the component hard drive to the backup device. Because the initial software does not contain the various configuration and setup information loaded into the component on site, a backup will save considerable time in restoring a component to operational status in the event of a failure. A failure that would require the use of a backup for restoration would most likely be a complete failure of the hard drive. In most other failures, a restart of the system will restore the component to normal operation. This procedure provides instructions pertaining to backing-up DMS components at the Navy LNOSC and using the backup media to restore component operations. This procedure applies to all Navy LNOSC'S.

**1702.1 LNOSC and LCC Windows NT Backups Procedures**

The following methodology is provided for NT Backups.

a. Set up tapes to perform backups for four weeks before writing over an old tape. Number them by week, day of the week, and a consecutive tape number.

b. Week 1 tapes are numbered 1-7, week 2 tapes 8-14, week 3 tapes 15-21, and week 4 tapes 22-28. After tape 28 (or set for day 28) is used, tape 1 will be used again. Each day the next number will be used. Should multiple tapes be required to backup a component, number the tape sets for day 1 as 1-1 and 1-2, for day 2 as 2-1 and 2-2, and so on.

c. The tape pattern runs Monday-Sunday with Monday being a Full backup and Tuesday through Sunday being Differential backups.

d. Backups should be done near to midnight, Universal Time Coordinated (UTC) (0000Z) on all days. If the backup software is programmed to run automatically, the components will display a warning 10 minutes prior to the start of a backup. The tape should be placed into the tape drive unit at least 10 minutes prior to backup.

e. The tapes should be located in a tape drive cabinet in a secure location, away from any electromagnetic fields. The tapes

should be separated by machine type and week. The tapes should be kept in order by day. An empty tape cartridge should be left in the cabinet so that it will not be lost so that it marks the place in the row where the tape will be returned.

### 1702.2 LNOSC AND LCC UNIX Backup Procedures

The following methodology is provided for UNIX backups.

a. The backup software should not be set up to run automatically. The system/backup administrator shall be responsible for verifying that backups are completed in accordance with guidance provided in the component's System Administrator' Guide.

b. Backups should be performed during off-peak times (typically between GM 0000Z and 0300Z.) Additional guidance may be incorporated in local SOP'S.

c. After six hours, ensure the backup has completed by checking `/users/common /backups/<mmddyy>[full]` and search for "run time". If a time in seconds is associated with the run time, then the backup was successful. If not, inform a system administrator.

To determine if the backup was successful:

- (1) Open an HP Term window.
- (2) Type `cd /users/common/backups` (this changes the directory to the backup directory).
- (3) Type `ll`. This displays a backup list of files with the last one being that of the current day.
- (4) Type `grep seconds` and highlight the current day's file. The results should appear in seconds. If the result does not appear in seconds, but another prompt is displayed, the backup file needs to be reviewed for completion and any errors that were received.
- (5) Type `vi` and highlight the current day's file.
- (6) Search by pressing `esc` and type `/fback`.
- (7) Type `n` for next until the end of the file. Look for any error messages, i.e., "write error" or "second tape needed", within the file. If the file states "backup complete" but with error, then it is safe to manually eject the tape.
- (8) Replace the tape with the next tape as necessary.

**1703. Restoration of a Component Using Backups**

The backup of a component copies the entire hard drive to the backup device. If the component is involved in message handling (e.g., an MTA or MFI), a failure requiring a complete restoration will have made messages in the system at the time of failure unrecoverable. A restoration using the backup will place messages undelivered at the time of the backup onto the restored system message queue. Users may report delays in message receipt and the LSM must be prepared to respond appropriately. Messages, which can not be recovered after a system failure, may also be traced; the LSM must utilize any available archives to determine whether a claim of non-delivery is valid and the message was lost in the failure.

Component restoration with backup media shall only after obtaining approval of the system administrator or other locally designated site personnel.

APPENDIX A

ACRONYMS

ACRONYMS

ACC	Area Control Center
ACP	Allied Communications Publication
ADMD	Administrative Management Domain
ADUA	Administrative Directory User Agent
AIG	Address Indicator Group
AIS	Automated Information System
AOR	Area of Responsibility
ASCII	American Standard Code For Information Interchange
ASM	Area System Manager
BMTA	Backbone Message Transfer Agent
C	Country
CA	Certification Authorities
CAA	Certificate Approving Authority
C&A	Certification and Authentication
CAD	Collective Address Designator
CAW	Certification Authority Workstation
CCB	Configuration Control Board
CCITT	International Telegraph and Telephone Consultative Committee
CKL	Compromised Key List
CM	Configuration Management
CMS	Communications Security Materiel System
CN	Common Name
CNO	Chief of Naval Operations
COMNAVCOMTELCOM	Commander, Naval Computer and Telecommunications Command
CONOPS	Concept of Operations
CPU	Central Processing Unit
CRL	Certificate Revocation List
CumStat	Cumulative Statistics Report
DA	Directory Administrator
DAA	Designated Approving Authorities
DADS	DII Asset Distribution System
DAP	Directory Access Protocol
DCMS	Director, Communications Security Materiel System
DCOC	DMS Central Operations Center
DDN	Directory Distinguished Name
DDN	Defense Data Network
DDT	Detailed Design Tool
DIB	Directory Information Base
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISAC	DISA Circular
DISA-EUR	DISA-Europe
DISA-PAC	DISA-Pacific
DISN	Defense Information Systems Network
DISP	Directory Information Shadowing Protocol
DIT	Directory Information Tree



DITSCAP Defense Information Technology Security Certification  
And Accreditation Process

DMDS Defense Message Dissemination Subsystem

DMS Defense Message System

DN Distinguished Name

DoD Department of Defense

DoN Department of the Navy

DSA Directory System Agent

DSN Defense Switched Network

DSP Directory System Protocol

DTH Defense Message System Transition Hub

DUA Directory User Agent

DVT Design Validation Team

ECP Engineering Change Proposal

ECP Emergency Change Procedure

ECP Emergency Command Precedence

E-Mail Electronic Mail

FEN Field Engineering Notice

FOC Final Operational Capability

FISP Functional, Integration, Security, and Performance

FTP File Transfer Protocol

GDSA Global Directory System Agent

GENSER General Service

GNOSC Global Network Operations and Security Center

GSM Global System Manager

GWS GroupWare Server

HAG High Assurance Guard

HAZCON Hazardous Condition

HD Help Desk

ID Identification/Identity

IDUA Integrated Directory User Agent

IOC Initial Operational Capability

IP Interim Procedure

IPN Interim Procedure Notice

ISO International Organization for Standardization

ISP Implementation Strategy and Plan

ISSM Information Systems Security Manager

ISSO Information Systems Security Officer

ITU-TSS International Telecommunication Union  
Telecommunication Standardization Sector  
(formerly CCITT)

JANAP Joint Army/Navy/Air Force Procedures

JCS Joint Chiefs of Staff

JITC Joint Interoperability Test Center

KEA Key Exchange Algorithm

KMID Keying Material Identifier

KRL KMID Revocation List

LANT	Atlantic
LCC	Local Control Center
LDSA	Local Directory System Agent
LMTA	Local Message Transfer Agent
LNOSC	Local Network Operations and Security Center
LSM	Local System Manager
MCEB	Military Communications-Electronics Board
MFI	Multifunction Interpreter
MGDSA	Master Global DSA
MHS	Message Handling System
MIB	Management Information Base
MISSI	Multi-Level Information System Security Initiative
MITNOC	Marine Corps Information Technology Network Operations Center
ML	Mail List
MLA	Mail List Agent
MLM	Mail List Manager
MMHS	Military Message Handling System
MMID	Military Message Identification
MOU	Memorandum of Understanding
MS	Message Store
MSDD	Master System Detailed Design
MSP	Message Security Protocol
MTA	Message Transfer Agent
MTS	Message Transfer System
MTSID	MTS Identifier
MWS	Management Workstation
N/A	Not Applicable; Not Available
NCTAMS	Naval Computer and Telecommunications Area Master Station
NAVCOMTELSTA	Naval Computer and Telecommunications Station
NDN	Non-Delivery Notice
NIPRNET	Non-secure Internet Protocol Router Network
NSA	National Security Agency
NTP	Naval Telecommunications Procedures
NTP	Network Time Protocol
OPS	Operations
O/R	Originator and Recipient
ORA	Organizational Registration Authority
ORA	Organizational Release Authority
OSA	Organizational System Administrator
OSI	Open Systems Interconnection
OSO	Organizational Security Officer
OU	Organizational Unit
PAA	Policy Approving Authority
PAB	Personal Address Book
PAC	Pacific
PCA	Policy Creation Authority

PCMCIA Personal Computer Memory Card International Association  
PGWS Primary GroupWare Server  
PIN Personal Identification Number  
PLA Plain Language Address  
PM Program Manager  
PMO Program Management Office  
POC Point of Contact  
PRMD Private Management Domain  
PUA DMS Profiling User Agent

RA Registration Authority  
RADAY Radio Day  
RCDB Routing Configuration Database  
RFC Request for Comments  
RN Regional Node  
ROMC Required Operational Messaging Characteristics  
RNOSC Regional Network Operations and Security Center  
RSM Regional System Manager  
RSS Remote Service Site

SECNAV Secretary of the Navy  
SGDSA Shadow Global DSA  
SIPRNET Secret Internet Protocol Route Network  
SMS Service Management System/Station  
SMTP Simple Message Transfer Protocol  
SNMP Simple Network Management Protocol  
SOP Standard Operating Procedures  
SRA Sub-Registration Authority  
SSL Secure Sockets Layer  
SSO Systems Security Officer  
SysStat System Status Report

TS/C Top Secret/Collateral  
TT Trouble Tickets

UA User Agent  
URL Universal Resource Locator  
USMC U.S. Marine Corps  
USN U.S. Navy  
UTC Universal Time Coordinated

WAN Wide Area Network  
WESTHEM Western Hemisphere  
WWW World Wide Web

X.500 Directory Services Protocol  
X.509 Certificate Template

APPENDIX B  
GLOSSARY OF TERMS

GLOSSARY OF TERMS

**Accreditation.** A formal declaration by the Designated Approving Authority (DAA) that the automated information system is approved to operate in a particular security mode by using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an automated information system; it is based on the certification process and other management considerations.

**Administrative Directory User Agent (ADUA).** A software function, which provides the means whereby an authorized person can enter, modify, or delete data in the Directory Information Base.

**Authentication.** Establishes the validity of a claimed identity (e.g., workstation, originator, individual, user, device, or other entity in a system). Authentication verifies the identity of a communicating peer entity and the source of data.

**Certificate.** The public keys of a user, together with other information, rendered unforgeable by encipherment with the secret key of the certification authority that issued it.

**Certification.** a) The formal technical evaluation of security features and other safeguards of an Automated Information System (AIS). Certification supports the accreditation process and establishes the extent to which a particular AIS design and implementation meet a set of specified security requirements. b) The process of placing user certificates into the Directory. This is necessary for the functioning of MISSI security system.

**Component.** The existing or proposed hardware and software implementation of a DMS messaging application.

**Component Approval.** Action taken by the DMS management structure to allow implementation and operation of a component resulting from a DMS approved project.

**Configuration Management.** A discipline applying technical and administrative direction and surveillance to: a) identify and document the functional and physical characteristics of a configuration item, b) control changes to those characteristics, and c) record and report changes to processing and implementation status.

**Defense Information Infrastructure (DII).** A seamless web of communications networks, computers, software, databases, applications, and other capabilities that meets the information processing and transport needs of DoD users in peace and in all crises, conflict, humanitarian support, and wartime roles.

**Defense Information Systems Network (DISN).** The full set of DoD long-haul networks, both packet-switched and underlying communications transmission systems. DISN is a subset of DII.

It is the DoD'S consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner.

**Defense Message System (DMS)**. All hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between organizations and individuals in the DoD. The DMS relies on but does not include the Defense Data Network (DDN) and DISN.

**Designated Approving Authority (DAA)**. The official who has the authority to accept the security safeguards prescribed for an automated information system or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

**Directory Distinguished Name (DDN)**. A unique and unambiguous directory name that is composed of a sequence of relative distinguished names (RDN) indicating the path derived from the directory tree structure from the root to the named node. It can also be described as the name of the superior node combined with the RDN.

**Directory Name**. A Directory name is one component of an Originator/Recipient (O/R) name. It is the name of an entry in a Directory. In the context of message handling, the entry in the Directory will enable the O/R address to be retrieved for submission of a message.

**Directory Systems Agent**. The Directory Systems Agent serves to retain and make available part of the Directory Information Base. It is accessed by any component requiring Directory information by means of a Directory User Agent (DUA). Communication between the DUA and the DSA is via Directory Access Protocol (DAP).

**Directory User Agent (DUA)**. The DMS DUA allows the DMS writer or reader to query, interrogate, and administer the information in the DMS X.500 Directory Information Base (DIB). The DUA stores and allows updates to a limited local cache of commonly used DMS directory names and O/R addresses for use by the collocated DMS UA.

**Domain Defined Attribute (DDA)**. Optional attributes of an O/R address allocated to names within a management domain. DMS will use the following DDAs: ORA, RFC-822, PMSP-822, ACP-PLAD, and ACP-RI.

**Electronic Mail (E-Mail)**. The electronic generation, transmission, and display of correspondence and documents.

**File Transfer Protocol.** A protocol used by a TCP/IP application program to transfer files from one computer to another. It is commonly used on the Internet. The abbreviation FTP is sometimes used to mean the file transfer program itself.

**Firewall.** A type of access control gateway which is placed between a private or restricted access network and a public network to selectively filter incoming and/or outgoing traffic. Firewalls enhance network and application security.

**Fortezza.** A Personal Computer Memory Card International Association (PCMCIA) smart card that includes National Security Agency (NSA)-developed security mechanisms and interfaces with the MISSI software to protect DMS messages.

**Full Operational Capability (FOC).** a) At the system level, FOC is the point at which a fielded system fully meets the technical and operational specifications of the requirements documentation. FOC of a system may also be declared with exceptions agreed to by the Program Manager, the User, and the O&M activity. b) At the site level, FOC is the point at which the portion of the system at that site fully meets the technical and operations specifications of the requirements documentation. FOC for the site may also be declared with exceptions agreed to by the Program Manager, the site manager, and the O&M activity.

**Information.** Any communication or representation of knowledge in any medium or form.

**Infrastructure.** A backbone made up of interconnected DMS Government Open System Interconnection Profile (GOSIP) components to provide reliable, secure, and timely application services including messaging, directory, and management for users worldwide.

**Initial Operational Capability (IOC).** a) At the system level, IOC is the point at which some portion of the technical and operational specifications defined by the requirements documents have been achieved. The specific definition of IOC will vary for each system and would be negotiated among the Project Manager, the User, and the O&M activity. b) At the site level, IOC is the point at which the technical and operational specifications of that portion of the system installed at a specific site meet the documented requirements, but some portion of testing and/or conformance to be accomplished. The definition of IOC may be site specific and would be negotiated among the Project Manager, the Site Manager, and the O&M activity.

**Interface.** A connecting link or interrelationship between two systems or two devices, or between a user and an application, device or system. In the OSI reference model, it is the boundary between adjacent layers.

**International Organization for Standardization (ISO)**. An organization that establishes international standards for (among other things) computer network architecture. Membership is by country with 90 countries participating. The ISO Open Systems Interconnection Reference Model divides network functions into seven layers.

**Internet**. The collection of networks and gateways that use the TCP/IP protocol suite and function as a single, cooperative virtual network with near-universal connectivity. There are three levels of network services - unreliable connectionless packet delivery, reliable full duplex stream delivery, and application-level services like electronic mail that build on the first two.

**Internet Protocol (IP)**. Standard that allows dissimilar hosts to connect to each other through the Internet.

**Interoperability**. The ability of two or more systems or components to exchange and use information or services, so that they will operate effectively together.

**Local Area Network (LAN)**. A data network, usually located on its users' premises, within a limited geographical area.

**Mail List (ML)**. An X.400 O/R name that represents a defined group of DMS users. Mail List members include O/R names for DMS users or O/R names for other Mail Lists. The point of list expansion distinguishes a Mail List (expanded by an MLA) from a Distribution List (expanded in an MTA) and from an Address List (expanded in a UA). This clarification applies to usage in this document; usage is not standardized and may differ in other documents.

**Mail List Agent (MLA)**. The MLA receives messages addressed to Mail Lists for which the MLA is responsible. The DMS MLA is required to simplify the distribution of single messages to multiple recipients and to expand the Mail List to its individual members, generate the security tokens for each member, provide alternate delivery, and resubmit the new messages into the DMS MTS. The MLA also authenticates and encrypt all received messages as well as signs and encrypts all outgoing messages.

**Management Workstation (MWS)**. The MWS'S are utilized to effect management functions over all of the DMS components and intercommunications between MWS'S.

**Message Handling System (MHS)**. The collection of components that enable users to exchange messages on a store-and-forward basis. An MHS is composed of a variety of interconnected functional entities including Message Transfer Agents (MTA'S), Message Stores (MS'S), and User Agents (UA'S).



**Message Store (MS)**. The DMS MS is a user component that can serve as an intermediary between the DMS UA and the DMS MTA. When the supported DMS UA is "off-line", the DMS MS will store the received messages until the supported DMS UA is back "on-line". The DMS UA then queries the DMS MS for stored message status.

**Message Transfer Agent (MTA)**. Serves as the backbone component of the DMS Infrastructure, routing X.400 messages submitted by DMS UA'S to the next MTA, or one of its associated UA'S in accordance with the instructions contained on the X.400 message envelope.

**Message Transfer System (MTS)**. One or more MTA'S that provide the transfer between UA'S, MS'S, and DMS MLA'S.

**Minimize**. A state of emergency assigned to an area and all recipients in that area that requires all message originators to determine if each message is essential enough to burden network resources supporting that area. The resulting reduction of message traffic minimized delays for essential traffic.

**MISSI**. Multi-level Information System Security Initiative. MISSI software uses information on the PCMCIA Fortezza cards to implement end-to-end security mechanisms and provide a standard application interface to DMS components.

**Multi-chaining**. Used by one DSA to pass on a query to multiple DSA'S in the expectation that one or more DSA'S may be able to satisfy the request. Only the DSA that is able to continue to process the request will do so. The final results would be sent back to the originating DSA in order to satisfy the DUA query.

**Multifunction Interpreter (MFI)**. The MFI is responsible for providing interoperability among DMS baseline systems during transition to the DMS Target Architecture. The MFI provides message exchange capabilities among DTH legacy systems and electronic mail (E-mail) systems and DMS X.400-compliant component systems.

**Network**. In messaging, a system of connected relay points; a system of connected computers.

**Network Management**. The surveillance and control of the traffic across a network. Network management encompasses the techniques and organization needed to ensure service to network users even under adverse conditions, such as abnormal loads or equipment failures.

**Open Systems**. A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software a) to be ported with minimal changes across a wide range of systems, b) to inter-operate with other applications on local and remote

systems, and c) to interact with users in a style that facilitates user portability.

**Open Systems Interconnection (OSI)**. A classification of standards for promoting global connectivity. OSI standards are generally promulgated by the ISO and used by a variety of standards-setting bodies.

**Operations Message (Account)**. A DMS organizational message transferred between ACC'S/LCC'S, DTH'S, and RNOSC'S for the purpose of exchanging DMS operations related information. An Operations Message Account is an organizational message account set up for the purpose of sending and receiving operations messages.

**Organizational Message**. A message that includes command and control traffic and messages exchanged between organizational elements. These messages require release by the sending organization and distribution determination by the receiving organization. Due to their official and sometimes critical nature, such messages impose operational requirements on the communications systems for capabilities such as non-routine precedence, guaranteed timely delivery, high availability and reliability, and a specified level of survivability.

**Originator/Recipient (O/R) Address**. An attribute list that distinguishes one user or Mail List from another and identifies the user's point of access to the MHS or the distribution list's expansion point.

**Originator/Recipient (O/R) Name**. An identifier which a user can be designated as the originator, or a user can be designated as a potential recipient of a message. An O/R name distinguishes one user or Mail List from another. An O/R name is composed of a directory name and an O/R address. Each user will have one or more O/R name(s).

**OSI Reference Model**. The seven-layer model, defined by ISO, that provides the framework for building an open network. The seven layers, ranging from highest to lowest, are application, presentation, session, transport, network, data link, and physical.

**Packet Switching**. Data transmission process that uses addressed packets, each with its own routing, sequencing, and error-checking information. This allows a channel to be shared by many users, since the circuit is required only for the time it takes to send a single packet.

**Plain Language Address (PLA)**. The plain language representation of a DTH legacy user's organization, geographical location, and office symbol.

**Precedence.** Reflection of the originator's determination of the required rapidity of delivery of the message (i.e., Critic, ECP, Flash, Immediate, Priority, Routine). Precedence determines the required speed of service and its associated message handling by the recipient(s).

**Priority.** Refers to the X.400 defined Grade of Delivery selection in the MTS.

**Profiling User Agent (PUA).** Provides messaging support to organizational users by representing a single organization's O/R Address. The PUA can be used for message archiving and retrieval tools for monitoring system integrity, message logging, and automatic combination of sectionalized DTH legacy messages. The PUA automatically assigns distribution to a message based on profiles defined for the end users within an organization.

**Project Approval.** The action taken by the DMS Management Structure to establish a DMS project for development and/or acquisition.

**Protocol.** Hardware and software procedures used to control the transfer of data in communications networks and between networks and subscriber equipment.

**Recipient.** A user (i.e., a person, Mail List, or component of the message handling environment) that receives a message. This includes the recipient that the originator specifies as the intended destination of a message, and the one who receives the message after all possible redirection.

**Release Authority.** A designated authority, or an automated process accredited by a Designated Approving Authority, within an organization, that has approval authority to release organizational messages.

**Replication.** The duplication of directory information from one DSA onto another DSA (or other component). Two methods are shadowing, which is defined by the X.500 series and caching, which is locally defined and nonstandard.

**Risk Management.** The total process of identifying, measuring, and minimizing uncertain events affecting automated information system resources. It includes risk analysis, cost-benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.

**Routing Indicator (RI).** A group of letters, used in Allied Communications Publication (ACP) 127, and Joint Army, Navy, and Air Force Procedures (JANAP) 128 messaging, assigned to identify a station within a network to facilitate routing of traffic. The RI indicates the status of the station, and may indicate its geographical area. RI'S are composed in accordance with the Routing Indicator Plan described in the ACP 121 series, and are

used to define the network address of a Telecommunications Center (TCC) serving one or more organizations.

**Security Certification.** The formal technical evaluation of security features and other safeguards of an AIS. Certification, which supports the accreditation process, establishes the extent to which a particular automated information system design and implementation meet a set of specified security requirements.

**Service Provider.** Any entity providing a service, especially a communications service. In the OSI reference models, the resource that provides the facilities of the relevant OSI Reference Model layer. The OSI session and transport layers are the service providers for the session and transport services, and the X.25 network gateway or X.25 message control system is the service provider for the network service.

**Service Provisioning.** Those activities necessary to initiate or modify messaging and directory services to a customer. In the OSI reference models, the providing of layers that provide facilities for the associated services.

**Shadowing.** A method by which directory information is replicated (duplicated) between a supplier and consumer DSA.

**Simple Mail Transfer Protocol (SMTP).** A TCP/IP protocol for transferring electronic mail messages from one host to another. SMTP specifies how two mail systems interact and the format of control messages they exchange to transfer mail.

**Simple Network Management Protocol (SNMP).** A standard protocol used to monitor IP gateways and the networks to which they attach.

**System.** People, machines, and methods organized to accomplish a set of specific functions.

**TCP/IP Gateway.** A device or pair of devices used to interconnect two or more networks or sub-networks, enabling the passage of data from one to another. In this architecture, a gateway contains an IP module and, for each connected sub-network, sub-network protocol module. The routing protocol is used to coordinate with other gateways. A gateway is often called an IP router.

**Terminal.** A device, instrument or facility used to generate, transmit, and receive message traffic via a transmission line from another terminal or from a network.

**Universal Time Coordinated (UTC).** The mean solar time of the meridian of Greenwich, England, used as the prime basis of standard time throughout the world (Greenwich mean time).

User. 1) any person, organization, or functional unit using the services of an information processing system; 2) in a conceptual schema language, a person or process that may issue or receive commands or messages to or from the information system.

User Agent (UA). The UA is the user component of the system. It must interface with the DMS MHS on behalf of a single DMS user or organization writer or reader. The UA must prepare message receipt notifications, store messages, and maintain writer-to-reader accountability.

X.400. The international recommendations developed by ITU-T for a store-and-forward message handling system in a multi-vendor environment.

X.500. The international recommendations developed by ITU-T for directory services or electronic mail.

X.509. An X.509 certificate is a structure of information that ties the user identity with the user's public key

APPENDIX C

DON LNOSC LOCATIONS

DON LNOSC LOCATIONS

NCTAMS PAC SBU DMS LNOSC OPERATIONS ROLES	
PLA	ACC HONOLULU HI(n)
LNOSC TYPE	DMS Area Control Center (ACC)
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-453-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(n)/ou=ACC Honolulu HI(n)
ROLE	Sub-Registration Authority
PLA	SUBREGAUTH HONOLULU(n)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-453-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(n)/ou=ACC Honolulu HI(n)/cn=SUBREGAUTH HONOLULU(n)
ROLE	Certificate Authority
PLA	CERTAUTH0002 (U-NCTAMS PAC Wahiawa HI)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=Dod/ou=Navy/cn=CERTAUTH0002 (U-NCTAMS PAC Wahiawa HI)
ROLE	Help Desk

<b>NCTAMS PAC SBU DMS LNOSC OPERATIONS ROLES</b>	
PLA	HELPDESK HONOLULU(n)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(n)/ou=ACC Honolulu HI(n)/cn=HELP DESK HONOLULU(n)
ROLE	DMS Operations Manager
PLA	DMSOPSMNGR HONOLULU(n)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(n)/ou=ACC Honolulu HI(n)/cn=DMSOPSMNGR HONOLULU(n)
ROLE	Area System Manager
PLA	ASM HONOLULU(n)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(n)/ou=ACC Honolulu HI(n)/cn=ASM HONOLULU(n)
ROLE	Directory Administrator
PLA	Directory Manager HHI(n)
POC	



<b>NCTAMS PAC SBU DMS LNOSC OPERATIONS ROLES</b>	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(n)/ou=ACC Honolulu HI(n)/cn=Directory Manager HHI(n)
ROLE	Mail List Manager
PLA	MLMANAGER HONOLULU(n)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(n)/ou=ACC Honolulu HI(n)/cn=MLMANAGER HONOLULU(n)
ROLE	Mail List Administrator
PLA	
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	
ROLE	Configuration Manager
PLA	CONFIGMNGR HONOLULU(n)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786

<b>NCTAMS PAC SBU DMS LNOSC OPERATIONS ROLES</b>	
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(n)/ou=ACC Honolulu HI(n)/cn=CONFIGMNGR HONOLULU(n)
ROLE	Security Officer
PLA	SECURITY OFFICER HONOLULU(n)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(n)/ou=ACC Honolulu HI(n)/cn=SECURITY OFFICER HONOLULU(n)

NCTAMS PAC SIPRNET DMS LNOSC OPERATIONS ROLES	
PLA	ACC HONOLULU HI(S)
LNOSC TYPE	DMS Area Control Center (ACC)
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653- 0746      FAX: (808)653- 5324      DSN: 315-453- 0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(s)/ou=ACC Honolulu HI(s)
ROLE	Sub-Registration Authority
PLA	SUBREGAUTH HONOLULU(s)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653- 0746      FAX: (808)653- 5324      DSN: 315-453- 0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(s)/ou=ACC Honolulu HI(s)/cn=SUBREGAUTH HONOLULU(s)
ROLE	Certificate Authority
PLA	CERTAUTH0007 (S-NCTAMS PAC Wahiawa HI)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653- 0746      FAX: (808)653- 5324      DSN: 315-653- 0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=Dod/ou=Navy/cn=CERTAUTH0007 (S-NCTAMS PAC Wahiawa HI)
ROLE	Help Desk
PLA	HELPDESK HONOLULU(s)
POC	

<b>NCTAMS PAC SIPRNET DMS LNOSC OPERATIONS ROLES</b>	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(s)/ou=ACC Honolulu HI(s)/cn=HELP DESK HONOLULU(s)
ROLE	DMS Operations Manager
PLA	DMSOPSMNGR HONOLULU(s)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(s)/ou=ACC Honolulu HI(s)/cn=DMSOPSMNGR HONOLULU(s)
ROLE	Area System Manager
PLA	ASM HONOLULU(s)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(s)/ou=ACC Honolulu HI(s)/cn=ASM HONOLULU(s)
ROLE	Directory Administrator
PLA	Directory Manager HI(s)
POC	

<b>NCTAMS PAC SIPRNET DMS LNOSC OPERATIONS ROLES</b>	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746    FAX: (808)653-5324    DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(s)/ou=ACC Honolulu HI(s)/cn=Directory Manager HI(s)
ROLE	Mail List Manager
PLA	MLMANAGER HONOLULU(s)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746    FAX: (808)653-5324    DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(s)/ou=ACC Honolulu HI(s)/cn=MLMANAGER HONOLULU(s)
ROLE	Mail List Administrator
PLA	N/A IAW 162130ZMAR00
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746    FAX: (808)653-5324    DSN: 315-653-0746
E-MAIL	
X.500	
ROLE	Configuration Manager
PLA	CONFIGMNGR HONOLULU(s)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786

<b>NCTAMS PAC SIPRNET DMS LNOSC OPERATIONS ROLES</b>	
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(s)/ou=ACC Honolulu HI(s)/cn=CONFIGMNGR HONOLULU(s)
ROLE	Security Officer
PLA	SECURITY OFFICER HONOLULU(s)
POC	
ADDRESS	NCTAMS PAC WAHIAWA 500 CENTER STREET WAHIAWA HI, 96786
PHONE/FAX	Comm: (808)653-0746      FAX: (808)653-5324      DSN: 315-653-0746
E-MAIL	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=HONOLULU/ou=NCTAMSPAC HONOLULU HI(s)/ou=ACC Honolulu HI(s)/cn=SECURITY OFFICER HONOLULU(s)

<b>NCTAMSLANT NORFOLK, VA DMS LNOSC OPERATIONS ROLES</b>	
PLA	NCTAMSLANT NORFOLK VA
LNOSC TYPE	AREA CONTROL NETWORK OPERATION AND SECURITY CENTER (ACC)
ADDRESS	9625 Moffett Ave Norfolk Va 23511-2784
PHONE/FAX	Comm: 757-444-      FAX: 757-444-      DSN: 564-7346 7346                      3578
E-MAIL	
X.500	OU=NCTAMS LANT Norfolk Va(N);OU=ACC Norfolk Va(n);cn=OU=NCTAMS LANT Norfolk Va(N);OU=ACC Norfolk Va(n)
ROLE	Sub-Registration Authority
PLA	NCTAMSLANT NORFOLK VA
POC	EARNEST L BESS
ADDRESS	SAME AS PARA 1 ABOVE
PHONE/FAX	Comm: 757-445-      FAX: 757-444-      DSN: 565-1163 1163                      3578
E-MAIL	BESSE@DMSLANT.NAVY.MIL
X.500	OU=NCTAMS LANT Norfolk Va(n);OU=ACC Norfolk Va(n);cn=SUBREGAUTH Norfolk Va(n)
ROLE	Certificate Authority
PLA	NCTAMSLANT NORFOLK VA
POC	GRATIA L. PATTERSON
ADDRESS	SAME AS PARA 1 ABOVE
PHONE/FAX	Comm: 757-445-      FAX: 757-444-      DSN: 565-1163 1163                      3578
E-MAIL	PATTERSONG@DMSLANT.NAVY.MIL
X.500	OU=NCTAMS LANT Norfolk Va(n);OU=ACC Norfolk Va(n);cn=CERTAUTH0001 (U-NCTAMS LANT NORFOLK VA)
ROLE	Help Desk
PLA	NCTAMSLANT NORFOLK VA
POC	IT1 BRYANT K LAW
ADDRESS	SAME AS PARA 1 ABOVE

<b>NCTAMSLANT NORFOLK, VA DMS LNOSC OPERATIONS ROLES</b>	
PHONE/FAX	Comm: 757-444-8478 FAX: 757-444-3578 DSN: 564-8478
E-MAIL	LAWB@DMSLANT.NAVY.MIL
X.500	OU=NCTAMS LANT Norfolk Va(n);OU=ACC Norfolk Va(n);cn=HELPDESK Norfolk Va(n)
ROLE	DMS Operations Manager
PLA	NCTAMSLANT NORFOLK VA
POC	EDWARD DUFF
ADDRESS	SAME AS PARA 1 ABOVE
PHONE/FAX	Comm: 757-444-7346 FAX: 757-444-3578 DSN: 564-7346
E-MAIL	DUFFE@DMSLANT.NAVY.MIL
X.500	OU=NCTAMS LANT Norfolk Va(n);OU=ACC Norfolk Va(n);cn=DMSOPMNGR Norfolk Va(n)
ROLE	Area System Manager
PLA	NCTAMSLANT NORFOLK VA
POC	AUGUSTO TORRES
ADDRESS	SAME AS PARA 1 ABOVE
PHONE/FAX	Comm: 757-444-3039 FAX: 757-444-0039 DSN: 564-3039
E-MAIL	TORRESA@NCTAMSLANT.NAVY.MIL
X.500	OU=NCTAMS LANT Norfolk Va(n);OU=ACC Norfolk Va(n);cn=ASM Norfolk Va(n)
ROLE	Directory Administrator
PLA	NCTAMSLANT NORFOLK VA
POC	IT2 VICTOR A WHITEHEAD
ADDRESS	SAME AS PARA 1 ABOVE
PHONE/FAX	Comm: 757-444-7346 FAX: 757-444-3578 DSN: 564-7346
E-MAIL	WHITEHEADV@DMSLANT.NAVY.MIL
X.500	OU=NCTAMS LANT Norfolk Va(n);OU=ACC Norfolk Va(n);cn=DIRADMIN5 Norfolk Va(n)
ROLE	Mail List Manager
PLA	NCTAMSLANT NORFOLK VA
POC	IT2 MICHAEL A FERROL



NCTAMSLANT NORFOLK, VA DMS LNOSC OPERATIONS ROLES	
ADDRESS	SAME AS PARA 1 ABOVE
PHONE/FAX	Comm: 757-444-8478 FAX: 757-444-3578 DSN: 564-8478
E-MAIL	FERROLM@DMSLANT.NAVY.MIL
X.500	OU=NCTAMS LANT Norfolk Va(n);OU=ACC Norfolk Va(n);cn=MLMANAGER Norfolk Va(n)
ROLE	Mail List Administrator
PLA	NCTAMSLANT NORFOLK VA
POC	NOT BEING USED AT THIS TIME
ADDRESS	SAME AS PARA 1 ABOVE
PHONE/FAX	Comm: FAX: DSN:
E-MAIL	
X.500	OU=NCTAMS LANT Norfolk Va(n);OU=ACC Norfolk Va(n);cn=MLADMIN1 Norfolk Va(n)
ROLE	Configuration Manager
PLA	NCTAMSLANT NORFOLK VA
POC	EDWARD DUFF
ADDRESS	SAME AS PARA 1 ABOVE
PHONE/FAX	Comm: 757-444-7346 FAX: 757-444-3578 DSN: 564-7346
E-MAIL	DUFFE@DMSLANT.NAVY.MIL
X.500	OU=NCTAMS LANT Norfolk Va(n);OU=ACC Norfolk Va(n);cn=CONFIGMNGR Norfolk Va(n)
ROLE	Security Officer
PLA	NCTAMSLANT NORFOLK VA
POC	MATTHEW J ROSENTHAL
ADDRESS	SAME AS PARA 1 ABOVE
PHONE/FAX	Comm: 757-444-8478 FAX: 757-444-3578 DSN: 564-8478
E-MAIL	ROSENTHALM@DMSLANT.NAVY.MIL
X.500	OU=NCTAMS LANT Norfolk Va(n);ou=ACC Norfolk Va(n);cn=SECURITY OFFICER Norfolk Va(n)

NAVCOMTELSTA KEFLAVIK IC LNOSC (SBU) DMS LNOSC OPERATIONS ROLES	
PLA	NAVCOMTELSTA KEFLAVIK IC
LNOSC TYPE	LCC(SBU)
ADDRESS	PSC 1003 Box 22 FPO AE 09728-0322
PHONE/FAX	Comm: 354-425-2657      FAX: 450-4348/354-425-4348      DSN: 450-2657
E-MAIL	lcckeflavikn@dms-keflavik.navy.mil
X.500	c:US,o:U.S. Government,ou:DoD,ou:Navy,ou:Organizations,l:Iceland,l:Keflavik,ou:NAVCOMTELSTA KEFLAVIK IC(n),ou:LCC Keflavik IC(n)
ROLE	Sub-Registration Authority
PLA	NAVCOMTELSTA KEFLAVIK IC
POC	IT1 (SW) Shreve
ADDRESS	PSC 1003 Box 22 FPO AE 09728-0322
PHONE/FAX	Comm: 354-425-4581      FAX: 450-4348/354-425-4348      DSN: 450-4581
E-MAIL	shrevert@nctskef.navy.mil
X.500	c:US,o:U.S. Government,ou:DoD,ou:Navy,ou:Organizations,l:Iceland,l:Keflavik,ou:NAVCOMTELSTA KEFLAVIK IC(n),ou:LCC Keflavik IC(n),cn:SUBREGAUTH Keflavik(n)
ROLE	Certificate Authority
PLA	NAVCOMTELSTA KEFLAVIK IC
POC	IT2 Hughes
ADDRESS	PSC 1003 Box 22 FPO AE 09728-0322
PHONE/FAX	Comm: 354-425-2500      FAX: 450-4348/354-425-4348      DSN: 450-2500

NAVCOMTELSTA KEFLAVIK IC LNOSC (SBU) DMS LNOSC OPERATIONS ROLES	
E-MAIL	hughesj@nctskef.navy.mil
X.500	c:US,o:U.S. Government,ou:DoD,ou:Navy,ou:Organizations,l:Iceland,l:Keflavik,ou:NAVCOMTELSTA KEFLAVIK IC(n),ou:LCC Keflavik IC(n),cn:CERTAUTH Keflavik(n)
ROLE	Help Desk
PLA	NAVCOMTELSTA KEFLAVIK IC
POC	IT3 Thalhuber
ADDRESS	PSC 1003 Box 22 FPO AE 09728-0322
PHONE/FAX	Comm: 354-425-2657      FAX: 450-4348/354-425-4348      DSN: 450-2657
E-MAIL	thalhuberd@nctskef.navy.mil
X.500	c:US,o:U.S. Government,ou:DoD,ou:Navy,ou:Organizations,l:Iceland,l:Keflavik,ou:NAVCOMTELSTA KEFLAVIK IC(n),ou:LCC Keflavik IC(n),cn:HelpDesk Keflavik(n)
ROLE	DMS Operations Manager
PLA	NAVCOMTELSTA KEFLAVIK IC
POC	ITC (SW) Reeve
ADDRESS	PSC 1003 Box 22 FPO AE 09728-0322
PHONE/FAX	Comm: 354-425-7522      FAX: 450-4348/354-425-4348      DSN: 450-7522
E-MAIL	reeveh@nctskef.navy.mil
X.500	c:US,o:U.S. Government,ou:DoD,ou:Navy,ou:Organizations,l:Iceland,l:Keflavik,ou:NAVCOMTELSTA KEFLAVIK IC(n),ou:LCC Keflavik IC(n),cn:DMSOPSMNGR Keflavik(n)
ROLE	Area System Manager
PLA	NAVCOMTELSTA KEFLAVIK IC
POC	IT2 Ross

NAVCOMTELSTA KEFLAVIK IC LNOSC (SBU) DMS LNOSC OPERATIONS ROLES	
ADDRESS	PSC 1003 Box 22 FPO AE 09728-0322
PHONE/FAX	Comm: 354-425-      FAX: 450-      DSN: 450-2500 2500                      4348/354-425- 4348
E-MAIL	rossm@nctskef.navy.mil
X.500	c:US,o:U.S. Government,ou:DoD,ou:Navy,ou:Organizations,l:Iceland,l:Keflavik,ou:NAVCOMTELSTA KEFLAVIK IC(n),ou:LCC Keflavik IC(n),cn:LSM Keflavik(n)
ROLE	Directory Administrator
PLA	NAVCOMTELSTA KEFLAVIK IC
POC	IT3 Thalhuber
ADDRESS	PSC 1003 Box 22 FPO AE 09728-0322
PHONE/FAX	Comm: 354-425-      FAX: 450-      DSN: 450-2657 2657                      4348/354-425- 4348
E-MAIL	thalhuberd@nctskef.navy.mil
X.500	c:US,o:U.S. Government,ou:DoD,ou:Navy,ou:Organizations,l:Iceland,l:Keflavik,ou:NAVCOMTELSTA KEFLAVIK IC(n),ou:LCC Keflavik IC(n),cn:DIRADMIN Keflavik(n)
ROLE	Mail List Manager
PLA	NAVCOMTELSTA KEFLAVIK IC
POC	IT2 Ross
ADDRESS	PSC 1003 Box 22 FPO AE 09728-0322
PHONE/FAX	Comm: 354-425-      FAX: 450-      DSN: 450-2657 2657                      4348/354-425- 4348
E-MAIL	rossm@nctskef.navy.mil

<b>NAVCOMTELSTA KEFLAVIK IC LNOSC (SBU)</b> <b>DMS LNOSC OPERATIONS ROLES</b>	
X.500	c:US,o:U.S. Government,ou:DoD,ou:Navy,ou:Organizations,l:Iceland,l:Keflavik,ou:NAVCOMTELSTA KEFLAVIK IC(n),ou:LCC Keflavik IC(n),cn:MLMANAGER Keflavik(n)
ROLE	Mail List Administrator
PLA	NAVCOMTELSTA KEFLAVIK IC
POC	IT2 Ross
ADDRESS	PSC 1003 Box 22 FPO AE 09728-0322
PHONE/FAX	Comm: 354-425-2657      FAX: 450-4348/354-425-4348      DSN: 450-2657
E-MAIL	rossm@nctskef.navy.mil
X.500	c:US,o:U.S. Government,ou:DoD,ou:Navy,ou:Organizations,l:Iceland,l:Keflavik,ou:NAVCOMTELSTA KEFLAVIK IC(n),ou:LCC Keflavik IC(n),cn:MLADMIN Keflavik(n)
ROLE	Configuration Manager
PLA	NAVCOMTELSTA KEFLAVIK IC
POC	IT2 Ross
ADDRESS	PSC 1003 Box 22 FPO AE 09728-0322
PHONE/FAX	Comm: 354-425-2657      FAX: 450-4348/354-425-4348      DSN: 450-2657
E-MAIL	rossm@nctskef.navy.mil
X.500	c:US,o:U.S. Government,ou:DoD,ou:Navy,ou:Organizations,l:Iceland,l:Keflavik,ou:NAVCOMTELSTA KEFLAVIK IC(n),ou:LCC Keflavik IC(n),cn:CONFIGMNGR Keflavik(n)
ROLE	Security Officer
PLA	NAVCOMTELSTA KEFLAVIK IC
POC	ITC (SW) Cannon

NAVCOMTELSTA KEFLAVIK IC LNOSC (SBU) DMS LNOSC OPERATIONS ROLES	
ADDRESS	PSC 1003 Box 22 FPO AE 09728-0322
PHONE/FAX	Comm: 354-425-7437      FAX: 450-4348/354-425-4348      DSN: 450-7437
E-MAIL	cannonl@nctskef.navy.mil
X.500	c:US,o:U.S. Government,ou:DoD,ou:Navy,ou:Organizations,l:Ice land,l:Keflavik,ou:NAVCOMTELSTA KEFLAVIK IC(n),ou:LCC Keflavik IC(n),cn:Security Officer Keflavik(n)

NAVCOMSTEA WASHINGTON, DC DMS LNOSC OPERATIONS ROLES	
PLA	NAVCOMTELSTA WASHINGTON DC
LNOSC TYPE	LCC
ADDRESS	1325 10 <sup>TH</sup> SREET, SE BLDG 196  WASHINGTON NAVY YARD, DC 20374-5069
PHONE/FAX	Comm: 202-685-      FAX: 202-433-      DSN: 325-2404 2404                      0351
E-MAIL	
X.500	C=US/O=U.S. Government/ OU=DoD/ OU=Navy/OU=NAVCOMTELSTA WASHINGTON DC(n)/OU=LCC WASHINGTON DC(n)
ROLE	Sub-Registration Authority
PLA	NAVCOMTELSTA WASHINGTON DC
POC	CHRISTINE HESTER
ADDRESS	1325 10 <sup>th</sup> STREET, SE  WASHINGTON NAVY YARD, DC 20374-5069
PHONE/FAX	Comm: 202-685-      FAX: 202-433-      DSN: 325-2430 2430                      2472
E-MAIL	HESTERC@NCTSWASH.NAVY.MIL
X.500	C=US/O=U.S. Government/ OU=DoD/ OU=Navy/OU=NAVCOMTELSTA WASHINGTON DC(n)/OU=LCC WASHINGTON DC(n)/CN=SUBREGAUTH WASHINGTON(n)
ROLE	Certificate Authority
PLA	NAVCOMTELSTA WASHINGTON DC
POC	ITC(SW) CLARK SNEED
ADDRESS	1325 10 <sup>th</sup> STREET, SE  WASHINGTON NAVY YARD, DC 20374-5069
PHONE/FAX	Comm: 202-685-      FAX: 202-433-      DSN: 325-2427 2427                      0351
E-MAIL	SNEEDC@NCTSWASH.NAVY.MIL
X.500	C=US/O=U.S. Government/ OU=DoD/ OU=Navy/OU=NAVCOMTELSTA WASHINGTON DC(n)/OU=LCC WASHINGTON DC(n)/CN=CERTA0001 WASHINGTON(n)
ROLE	Help Desk
PLA	NAVCOMTELSTA WASHINGTON DC
POC	IT2 MAHONE SCOTT

<b>NAVCOMSTEA WASHINGTON, DC DMS LNOSC OPERATIONS ROLES</b>	
ADDRESS	1325 10 <sup>th</sup> STREET, SE  WASHINGTON NAVY YARD, DC 20374-5069
PHONE/FAX	Comm: 202-685-      FAX: 202-433-      DSN: 325-2404 2404                      0368
E-MAIL	SCOTTM@NCTSWASH.NAVY.MIL
X.500	C=US/O=U.S. Government/ OU=DoD/ OU=Navy/OU=NAVCOMTELSTA WASHINGTON DC(n)/OU=LCC WASHINGTON DC(n)/CN=HELPDESK WASHINGTON(n)
ROLE	DMS Operations Manager
PLA	NAVCOMTELSTA WASHINGTON DC
POC	DAVID DAVIS
ADDRESS	1325 10 <sup>th</sup> STREET, SE  WASHINGTON NAVY YARD, DC 20374-5069
PHONE/FAX	Comm: 202-685-      FAX: 202-433-      DSN: 325-2431 2431                      0351
E-MAIL	DAVISD@NCTSWASH.NAVY.MIL
X.500	C=US/O=U.S. Government/ OU=DoD/ OU=Navy/OU=NAVCOMTELSTA WASHINGTON DC(n)/OU=LCC WASHINGTON DC(n)/CN=DMSOPSMNGR WASHINGTON (n)
ROLE	Area System Manager
PLA	NAVCOMTELSTA WASHINGTON DC
POC	LT MICHELLE HILLMEYER
ADDRESS	1325 10 <sup>th</sup> STREET, SE  WASHINGTON NAVY YARD, DC 20374-5069
PHONE/FAX	Comm: 202-685-      FAX: 202-433-      DSN: 325-2416 2416                      0351
E-MAIL	HILLMEYERM@NCTSWASH.NAVY.MIL
X.500	C=US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=NAVCOMTELSTA WASHINGTON DC(n)/OU=LCC WASHINGTON DC(n)/CN=ASM WASHINGTON(n)
ROLE	Directory Administrator
PLA	NAVCOMTELSTA WASHINGTON DC
POC	GARY PARKER
ADDRESS	1325 10 <sup>th</sup> STREET, SE  WASHINGTON NAVY YARD, DC 20374-5069
PHONE/FAX	Comm: 202-685-      FAX: 202-433-      DSN: 325-2419 2419                      0351



NAVCOMSTEA WASHINGTON, DC DMS LNOSC OPERATIONS ROLES	
E-MAIL	PARKERG@NCTSWASH.NAVY.MIL
X.500	C=US/O=U.S. Government/ OU=DoD/ OU=Navy/OU=NAVCOMTELSTA WASHINGTON DC(n)/OU=LCC WASHINGTON DC(n)/CN=DIRADMIN5 WASHINGTON(n)
ROLE	Mail List Manager
PLA	NAVCOMTELSTA WASHINGTON DC
POC	CHRISTINE HESTER
ADDRESS	1325 10 <sup>th</sup> STREET, SE  WASHINGTON NAVY YARD, DC 20374-5069
PHONE/FAX	Comm: 202-685-      FAX: 202-433-      DSN: 325-2430 2430                      2472
E-MAIL	HESTERC@NCTSWASH.NAVY.MIL
X.500	C=US/O=U.S. Government/ OU=DoD/ OU=Navy/OU=NAVCOMTELSTA WASHINGTON DC(n)/OU=LCC WASHINGTON DC(n)/CN=MLMANAGER WASHINGTON(n)
ROLE	Mail List Administrator
PLA	
POC	
ADDRESS	
PHONE/FAX	Comm:                      FAX:                      DSN:
E-MAIL	
X.500	
ROLE	Configuration Manager
PLA	NAVCOMTELSTA WASHINGTON DC
POC	DAVID DAVIS
ADDRESS	1325 10 <sup>th</sup> STREET, SE  WASHINGTON NAVY YARD, DC 20374-5069
PHONE/FAX	Comm: 202-685-      FAX: 202-433-      DSN: 325-2431 2431                      0351
E-MAIL	DAVISD@NCTSWASH.NAVY.MIL
X.500	C=US/O=U.S. Government/ OU=DoD/ OU=Navy/OU=NAVCOMTELSTA WASHINGTON DC(n)/OU=LCC WASHINGTON DC(n)/CN=CONFIGMNGR WASHINGTON(n)
ROLE	Security Officer
PLA	NAVCOMTELSTA WASHINGTON DC
POC	IT1(SW/AW) JERALD HOLLOMAN

<b>NAVCOMSTEA WASHINGTON, DC DMS LNOSC OPERATIONS ROLES</b>	
ADDRESS	1325 10 <sup>th</sup> STREET, SE  WASHINGTON NAVY YARD, DC 20374-5069
PHONE/FAX	Comm: 202-685-      FAX: 202-433-      DSN: 325-2429 2429                      0351
E-MAIL	HOLLOMANJ@NCTSWASH.NAVY.MIL
X.500	C=US/O=U.S. Government/ OU=DoD/ OU=Navy/OU=NAVCOMTELSTA WASHINGTON DC(n)/OU=LCC WASHINGTON DC(n)/CN=SECURITY OFFICER WASHINGTON(n)

NAVCOMTELSTA FAR EAST YOKOSUKA JA DMS LNOSC OPERATIONS ROLES	
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
LNOSC TYPE	LCC
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-743-8133
E-MAIL	lsmyokosuka@dms-yoko.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=JAPAN;l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(n)
ROLE	Sub-Registration Authority
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA (SRA NOT USED AT THIS COMMAND)
POC	IT1(SW) Roderick Reed
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-6502 311-473-6502      311-473-8133
E-MAIL	reedr@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=JAPAN;l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(n);ou=LCC Yokosuka JA(n);cn=SUBREGAUTH Yokosuka(n)
ROLE	Certificate Authority
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT1(SW) Roderick Reed
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-6502 311-473-6502      311-473-8133
E-MAIL	reedr@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;cn=CERTAUTH0010 (U-NCTS Far East Yokosuka JA)
ROLE	Help Desk
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA

NAVMCOMTELSTA FAR EAST YOKOSUKA JA DMS LNOSC OPERATIONS ROLES	
POC	LCC Watch Supervisor
ADDRESS	NAVMCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	MS Helpdesk@KSZNPE01.dms-yoko.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=JAPAN;l=YOKOSUKA; ou=NAVMCOMTELSTA FAR EAST YOKOSUKA JA(n);ou=LCC Yokosuka JA(n);cn=MS Helpdesk
ROLE	DMS Operations Manager
PLA	NAVMCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT2 Christopher Stanley
ADDRESS	NAVMCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	stanleyc@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=JAPAN;l=YOKOSUKA; ou=NAVMCOMTELSTA FAR EAST YOKOSUKA JA(n);ou=LCC Yokosuka JA(n);cn=DMSOPSMNGR Yokosuka(n)
ROLE	Area System Manager
PLA	NAVMCOMTELSTA FAR EAST YOKOSUKA JA
POC	Local Service Manager (LSM Account)
ADDRESS	NAVMCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	LSM Yokosukan@KSZNPE01.dms-yoko.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=JAPAN;l=YOKOSUKA; ou=NAVMCOMTELSTA FAR EAST YOKOSUKA JA(n);ou=LCC Yokosuka JA(n);cn=LSM Yokosuka(n)
ROLE	Directory Administrator
PLA	NAVMCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT2 Justin Kobielusz

NAVCOMTELSTA FAR EAST YOKOSUKA JA DMS LNOSC OPERATIONS ROLES	
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	kobieluszej@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=JAP AN;l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(n);ou=LCC Yokosuka JA(n);cn=DIRADMIN0001 Yokosuka(n)
ROLE	Mail List Manager
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT2 Justin Kobielusj
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	kobieluszej@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=JAP AN;l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(n);ou=LCC Yokosuka JA(n);cn=MLMANAGER Yokosuka(n)
ROLE	Mail List Administrator
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT2 Donald Nelson
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	nelsond@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=JAP AN;l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(n);ou=LCC Yokosuka JA(n);cn=MLMANAGER Yokosuka(n)
ROLE	Configuration Manager
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT2 Donald Nelson

NAVMOTELSTA FAR EAST YOKOSUKA JA DMS LNOSC OPERATIONS ROLES	
ADDRESS	NAVMOTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	nelsond@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=JAP AN;l=YOKOSUKA; ou=NAVMOTELSTA FAR EAST YOKOSUKA JA(n);ou=LCC Yokosuka JA(n);cn=CONFIGMNGR Yokosuka(n)
ROLE	Security Officer
PLA	NAVMOTELSTA FAR EAST YOKOSUKA JA
POC	ITC(SW) James Dobson
ADDRESS	NAVMOTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-9214 311-473-9214      311-473-8133
E-MAIL	dobsonj@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=JAP AN;l=YOKOSUKA; ou=NAVMOTELSTA FAR EAST YOKOSUKA JA(n);ou=LCC Yokosuka JA(n);cn=SECURITY OFFICER Yokosuka(n)

NAVCOMSTA FAR EAST YOKOSUKA JA DMS LNOSC OPERATIONS ROLES	
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
LNOSC TYPE	LCC
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-743-8133
E-MAIL	
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations(s);l= JAPAN(s);l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(s)
ROLE	Sub-Registration Authority
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA (SRA NOT USED AT THIS COMMAND)
POC	IT1(SW) Roderick Reed
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-6502 311-473-6502      311-473-8133
E-MAIL	reedr@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations(s);l= JAPAN(s);l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(n);ou=LCC Yokosuka JA(s);cn=SUBREGAUTH Yokosuka(s)
ROLE	Certificate Authority
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT1(SW) Roderick Reed
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-6502 311-473-6502      311-473-8133
E-MAIL	reedr@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;cn=CERTAUTH0010 (U- NCTS Far East Yokosuka JA)
ROLE	Help Desk
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA

<b>NAVCOMSTA FAR EAST YOKOSUKA JA DMS LNOSC OPERATIONS ROLES</b>	
POC	LCC Watch Supervisor
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	MS Helpdesk@KSZNPE01.dms-yoko.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations(s);l=JAPAN(s);l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(s);ou=LCC Yokosuka JA(s);cn=MS Helpdesk(s)
ROLE	DMS Operations Manager
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT2 Christopher Stanley
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	stanleyc@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations(s);l=JAPAN(s);l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(s);ou=LCC Yokosuka JA(s);cn=DMSOPSMNGR Yokosuka(s)
ROLE	Area System Manager
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	Local Service Manager (LSM Account)
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	LSM Yokosukan@KSZNPE01.dms-yoko.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations(s);l=JAPAN(s);l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(s);ou=LCC Yokosuka JA(s);cn=LSM Yokosuka(s)
ROLE	Directory Administrator
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT2 Justin Kobielusz



NAVCOMSTA FAR EAST YOKOSUKA JA DMS LNOSC OPERATIONS ROLES	
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	kobieluszej@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations(s);l=JAPAN(s);l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(s);ou=LCC Yokosuka JA(s);cn=DIRADMIN0001 Yokosuka(s)
ROLE	Mail List Manager
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT2 Justin Kobielusj
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	kobieluszej@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations(s);l=JAPAN(s);l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(s);ou=LCC Yokosuka JA(s);cn=MLMANAGER Yokosuka(s)
ROLE	Mail List Administrator
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT2 Donald Nelson
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	nelsond@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations(s);l=JAPAN(s);l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(s);ou=LCC Yokosuka JA(n);cn=MLMANAGER Yokosuka(s)
ROLE	Configuration Manager
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	IT2 Donald Nelson

NAVCOMSTA FAR EAST YOKOSUKA JA DMS LNOSC OPERATIONS ROLES	
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-3842 311-473-3842      311-473-8133
E-MAIL	nelsond@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations(s);l= JAPAN(s);l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(s);ou=LCC Yokosuka JA(s);cn=CONFIGMNGR Yokosuka(s)
ROLE	Security Officer
PLA	NAVCOMTELSTA FAR EAST YOKOSUKA JA
POC	ITC(SW) James Dobson
ADDRESS	NAVCOMTELSTA FAR EAST PSC 473 BOX 3  FPO, AP 96349-1800
PHONE/FAX	Comm: 011-81-      FAX: 011-81-      DSN: 243-9214 311-473-9214      311-473-8133
E-MAIL	dobsonj@nctsfe.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations(s);l= JAPAN(s);l=YOKOSUKA; ou=NAVCOMTELSTA FAR EAST YOKOSUKA JA(s);ou=LCC Yokosuka JA(s);cn=SECURITY OFFICER Yokosuka(s)

NCTAMS PAC DET OAHU SBU DMS LNOSC OPERATIONS ROLES	
PLA	NCTAMS PAC DET OAHU(n)
LNOSC TYPE	DMS LCC
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203 FAX: (808)477-5276 DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)
ROLE	Sub-Registration Authority
PLA	SUBREGAUTH OAHU(n)
POC	IT1(SW) Murakami
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203 FAX: (808)477-5276 DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=LSM OAHU(n)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=SUBREGAUTH OAHU(n)
ROLE	Certificate Authority
PLA	CERTAUTH0017 (U-NCTAMS PAC Det Oahu HI)
POC	IT1(SW) Murakami
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203 FAX: (808)477-5276 DSN: 315-453-3203

<b>NCTAMS PAC DET OAHU SBU DMS LNOSC OPERATIONS ROLES</b>	
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=LSM OAHU(n)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/cn=CERTHAUTH0017 (U-NCTAMS PAC Det Oahu HI)
ROLE	Help Desk
PLA	HELPDESK OAHU(n)
POC	IT1(SW) Sailiai
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203      FAX: (808)477-5276      DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=LSM OAHU(n)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=HELPDESK OAHU(n)
ROLE	DMS Operations Manager
PLA	DMSOPSMNGR OAHU(n)
POC	IT1(SW) Larry Rueb
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203      FAX: (808)477-5276      DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=LSM OAHU(n)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=DMSOPSMNGR OAHU(n)
ROLE	Area System Manager
PLA	LSM OAHU(n)
POC	IT1(SW) Larry Rueb

<b>NCTAMS PAC DET OAHU SBU DMS LNOSC OPERATIONS ROLES</b>	
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203    FAX: (808)477-5276    DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=LSM OAHU(n)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=LSM OAHU(n)
ROLE	Directory Administrator
PLA	Directory Manager OHI(n)
POC	IT1 Vann
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203    FAX: (808)477-5276    DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=LSM OAHU(n)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=Directory Manager OHI(n)
ROLE	Mail List Manager
PLA	MLMANAGER OAHU(n)
POC	IT2 Gaylor
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203    FAX: (808)477-5276    DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=LSM OAHU(n)

<b>NCTAMS PAC DET OAHU SBU DMS LNOSC OPERATIONS ROLES</b>	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=MLMANAGER OAHU(n)
ROLE	Mail List Administrator
PLA	
POC	
ADDRESS	
PHONE/FAX	Comm:                              FAX:                              DSN:
E-MAIL	
X.500	
ROLE	Configuration Manager
PLA	CONFIGMNGR OAHU(n)
POC	IT2 Gaylor
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI,            96816-4036
PHONE/FAX	Comm: (808)477-      FAX: (808)477-      DSN: 315-453- 3203                              5276                              3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=LSM OAHU(n)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=CONFIGMNGR OAHU(n)
ROLE	Security Officer
PLA	SECURITY OFFICER OAHU(n)
POC	IT1 Vann
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI,            96816-4036
PHONE/FAX	Comm: (808)477-      FAX: (808)477-      DSN: 315-453- 3203                              5276                              3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=LSM OAHU(n)

<b>NCTAMS PAC DET OAHU SBU DMS LNOSC OPERATIONS ROLES</b>	
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Haw aii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=SECURITY OFFICER OAHU(n)

<b>NCTAMS PAC SECRET DMS LNOSC OPERATIONS ROLES</b>	
PLA	NCTAMS PAC DET OAHU HI(S)
LNOSC TYPE	DMS LCC
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203    FAX: (808)477-5276    DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)
ROLE	Sub-Registration Authority
PLA	SUBREGAUTH OAHU(s)
POC	IT1(SW) Murakami
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203    FAX: (808)477-5276    DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=LSM OAHU(s)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=SUBREGAUTH OAHU(s)
ROLE	Certificate Authority
PLA	CERTAUTH0018 (S-NCTAMS PAC Det Oahu HI)
POC	IT1(SW) Murakami
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203    FAX: (808)477-5276    DSN: 315-453-3203



<b>NCTAMS PAC SECRET</b> <b>DMS LNOSC OPERATIONS ROLES</b>	
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Hawaii/l=OAHU/ou=NCTAMS PAC DET OAHU HI(n)/ou=RSS Oahu HI(n)/cn=LSM OAHU(n)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/cn=CERTHAUTH0018 (S-NCTAMS PAC Det Oahu HI)
ROLE	Help Desk
PLA	HELPDESK OAHU(s)
POC	IT1(SW) Sailiai
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203      FAX: (808)477-5276      DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=LSM OAHU(s)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=HELPDESK OAHU(s)
ROLE	DMS Operations Manager
PLA	DMSOPSMNGR OAHU(s)
POC	IT1(SW) Larry Rueb
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203      FAX: (808)477-5276      DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=LSM OAHU(s)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=DMSOPSMNGR OAHU(s)
ROLE	Area System Manager
PLA	LSM OAHU(s)
POC	IT1(SW) Larry Rueb

<b>NCTAMS PAC SECRET</b> <b>DMS LNOSC OPERATIONS ROLES</b>	
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203    FAX: (808)477-5276    DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=LSM OAHU(s)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=LSM OAHU(s)
ROLE	Directory Administrator
PLA	Directory Manager OHI(s)
POC	IT1 Vann
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203    FAX: (808)477-5276    DSN: 315-453-3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=LSM OAHU(s)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=Directory Manager OHI(s)
ROLE	Mail List Manager
PLA	MLMANAGER OAHU(s)
POC	IT2 Gaylor
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI, 96816-4036
PHONE/FAX	Comm: (808)477-3203    FAX: (808)477-5276    DSN: 315-453-3203

<b>NCTAMS PAC SECRET</b>	
<b>DMS LNOSC OPERATIONS ROLES</b>	
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=LSM OAHU(s)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=MLMANAGER OAHU(s)
ROLE	Mail List Administrator
PLA	
POC	
ADDRESS	
PHONE/FAX	Comm:                      FAX:                      DSN:
E-MAIL	
X.500	
ROLE	Configuration Manager
PLA	CONFIGMNGR OAHU(s)
POC	IT2 Gaylor
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI,        96816-4036
PHONE/FAX	Comm: (808)477-    FAX: (808)477-    DSN: 315-453- 3203                      5276                      3203
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=LSM OAHU(s)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=CONFIGMNGR OAHU(s)
ROLE	Security Officer
PLA	SECURITY OFFICER OAHU(s)
POC	IT1 Vann
ADDRESS	NCTAMS PAC DET OAHU HI BOX 64036 CAMP H. M. SMITH HONOLULU HI,        96816-4036
PHONE/FAX	Comm: (808)477-    FAX: (808)477-    DSN: 315-453- 3203                      5276                      3203

<b>NCTAMS PAC SECRET</b> <b>DMS LNOSC OPERATIONS ROLES</b>	
E-MAIL	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=LSM OAHU(s)
X.500	/c=us/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l=Hawaii(s)/l=OAHU/ou=NCTAMS PAC DET OAHU HI(s)/ou=RSS Oahu HI(s)/cn=SECURITY OFFICER OAHU(s)

NAVCOMM DET Chinhae Korea (N) DMS LNOSC OPERATIONS ROLES	
PLA	NAVCOMM DET CHINHAE KOR
LNOSC TYPE	RSS
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5384                      540-5830                      5384
E-MAIL	DELVALLEF@USFK.KOREA.ARMY.MIL
X.500	C=US / O=U.S. GOVERNMENT /OU=DoD /OU=NAVY /OU=ORGANIZATION/L=CHINHAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR (U-NCD Chinhae KO)
ROLE	Sub-Registration Authority
PLA	NAVCOMM DET CHINHAE KOR
POC	IT1 WILLARD SHEETS
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5403                      540-5830                      5403
E-MAIL	SHEETSW@USFK.KOREA.ARMY.MIL
X.500	C=US/O=U.S. GOVERNMENT/OU=DoD/OU=NAVY/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(n)/CN=SUBREGAUTH Chinhae (n)
ROLE	Certificate Authority
PLA	NAVCOMM DET CHINHAE KOR
POC	IT2 THOMAS MEINKE
ADDRESS	PSC 479 BOX 181 FPO AO 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5822                      540-5830                      5822
E-MAIL	MEINKET@USFK.KOREA.ARMY.MIL
X.500	C=US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(n) /CN=CERTAUTH0040 (U-NCD Chinhae KO)
ROLE	Help Desk
PLA	NAVCOMM DET CHINHAE KOR

NAVCOMM DET Chinhae Korea (N) DMS LNOSC OPERATIONS ROLES	
POC	IT1 PROVOST-WARREN
ADDRESS	PSC 479 BOX 181 FPO 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5822              540-5830              5822
E-MAIL	JACOBS@USFK.KOREA.ARMY.MIL
X.500	C=US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(n) /CN=HELPDESK Chinhae (n)
ROLE	DMS Operations Manager
PLA	NAVCOMM DET CHINHAE KOR
POC	CWO2 FELIX DEL VALLE
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540 5384              540-5830              5384
E-MAIL	DELVALLEF@USFK.KOREA.ARMY.MIL
X.500	C=US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(n)=RSS CHINHAE KOR(n)/CN=DMSOPSMNGR Chinhae(n)
ROLE	Area System Manager
PLA	NAVCOMM DET CHINHAE KOR
POC	ITC KENNETH REED
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5281              540-5830              5281
E-MAIL	REEDKR@USFK.KOREA.ARMY.MIL
X.500	C=US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(n)=RSS CHINHAE KOR(n)/CN=ASM Chinhae(n)
ROLE	Directory Administrator
PLA	NAVCOMM DET CHINHAE KOR
POC	ITC KENNETH REED

NAVCOMM DET Chinhae Korea (N) DMS LNOSC OPERATIONS ROLES	
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5281                      540-5830                      5281
E-MAIL	REEDKR@USFK.KOREA.ARMY.MIL
X.500	=US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(n)=RSS CHINHAE KOR(n)/CN=DIRADMIN Chinhae(n)
ROLE	Mail List Manager
PLA	NAVCOMM DET CHINHAE KOR
POC	IT2 CHRISTOPHER COTTS
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5822                      540-5830                      5822
E-MAIL	COTTSC@USFK.KOREA.ARMY.MIL
X.500	US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(n)=RSS CHINHAE KOR(n)/CN=MLMANAGER Chinhae(n)
ROLE	Mail List Administrator
PLA	N/A
POC	
ADDRESS	
PHONE/FAX	Comm:                      FAX:                      DSN:
E-MAIL	
X.500	
ROLE	Configuration Manager
PLA	N/A
POC	
ADDRESS	
PHONE/FAX	Comm:                      FAX:                      DSN:
E-MAIL	
X.500	
ROLE	Security Officer

NAVCOMM DET Chinhae Korea (N) DMS LNOSC OPERATIONS ROLES	
PLA	NAVCOMM DET Chinhae Kor
POC	IT1 BRUCE WIRFS
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5230              540-5830              5230
E-MAIL	WIRFSB@USFK.KOREA.ARMY.MIL
X.500	US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(n)=RSS CHINHAE KOR(n)/CN=SECURITY OFFICER Chinhae Kor (n)



NAVCOMM DET Chinhae Korea (N) DMS LNOSC OPERATIONS ROLES	
PLA	NAVCOMM DET Chinhae Kor
LNOSC TYPE	RSS
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5384              540-5830              5384
E-MAIL	DELVALLEF@USFK.KOREA.ARMY.MIL
X.500	C=US / O=U.S. GOVERNMENT /OU=DoD /OU=NAVY /OU=ORGANIZATION/L=CHINHAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR (S-NCD Chinhae KO)
ROLE	Sub-Registration Authority
PLA	NAVCOMM DET CHINHAE KOR
POC	IT1 WILLARD SHEETS
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5403              540-5830              5403
E-MAIL	SHEETSW@USFK.KOREA.ARMY.MIL
X.500	C=US/O=U.S. GOVERNMENT/OU=DoD/OU=NAVY/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(s)/CN=SUBREGAUTH Chinhae (n)
ROLE	Certificate Authority
PLA	NAVCOMM DET CHINHAE KOR
POC	IT2 THOMAS MEINKE
ADDRESS	PSC 479 BOX 181 FPO AO 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5822              540-5830              5822
E-MAIL	MEINKET@USFK.KOREA.ARMY.MIL
X.500	C=US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(s) /CN=CERTAUTH0040 (U-NCD Chinhae KO)
ROLE	Help Desk
PLA	NAVCOMM DET CHINHAE KOR
POC	IT1 PROVOST-WARREN

NAVCOMM DET Chinhae Korea (N) DMS LNOSC OPERATIONS ROLES	
ADDRESS	PSC 479 BOX 181 FPO 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5822              540-5830              5822
E-MAIL	JACOBS@USFK.KOREA.ARMY.MIL
X.500	C=US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(s) /CN=HELPDESK Chinhae (n)
ROLE	DMS Operations Manager
PLA	NAVCOMM DET CHINHAE KOR
POC	CWO2 FELIX DEL VALLE
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540 5384              540-5830              5384
E-MAIL	DELVALLEF@USFK.KOREA.ARMY.MIL
X.500	C=US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(s)=RSS CHINHAE KOR(n)/CN=DMSOPSMNGR Chinhae(s)
ROLE	Area System Manager
PLA	NAVCOMM DET CHINHAE KOR
POC	ITC KENNETH REED
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5281              540-5830              5281
E-MAIL	REEDKR@USFK.KOREA.ARMY.MIL
X.500	C=US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(s)=RSS CHINHAE KOR(n)/CN=ASM Chinhae(s)
ROLE	Directory Administrator
PLA	NAVCOMM DET CHINHAE KOR
POC	ITC KENNETH REED

NAVCOMM DET Chinhae Korea (N) DMS LNOSC OPERATIONS ROLES	
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5281              540-5830              5281
E-MAIL	REEDKR@USFK.KOREA.ARMY.MIL
X.500	=US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(s)=RSS CHINHAE KOR(n)/CN=DIRADMIN Chinhae(s)
ROLE	Mail List Manager
PLA	NAVCOMM DET CHINHAE KOR
POC	IT2 CHRISTOPHER COTTS
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5822              540-5830              5822
E-MAIL	COTTSC@USFK.KOREA.ARMY.MIL
X.500	US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(s)=RSS CHINHAE KOR(n)/CN=MLMANAGER Chinhae(s)
ROLE	Mail List Administrator
PLA	N/A
POC	
ADDRESS	
PHONE/FAX	Comm:                      FAX:                      DSN:
E-MAIL	
X.500	
ROLE	Configuration Manager
PLA	N/A
POC	
ADDRESS	
PHONE/FAX	Comm:                      FAX:                      DSN:
E-MAIL	
X.500	
ROLE	Security Officer

NAVCOMM DET Chinhae Korea (N) DMS LNOSC OPERATIONS ROLES	
PLA	NAVCOMM DET Chinhae Kor
POC	IT1 BRUCE WIRFS
ADDRESS	PSC 479 BOX 181 FPO AP 96269-1100
PHONE/FAX	Comm: 0553-82-      FAX: 0553-82-      DSN: 315-762- 540-5230              540-5830              5230
E-MAIL	WIRFSB@USFK.KOREA.ARMY.MIL
X.500	US/O=U.S. GOVERNMENT/OU=DoD/OU=Navy/OU=ORGANIZATION/L=CHIN HAE/L=KOREA/OU=NAVCOMM DET CHINHAE KOR(s)=RSS CHINHAE KOR(n)/CN=SECURITY OFFICER Chinhae Kor (s)

<b>NCTS Diego Garcia SBU DMS LNOSC OPERATIONS ROLES</b>	
PLA	NAVCOMTELSTA DIEGO GARCIA
LNOSC TYPE	DMS RSS
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Die go Garcia Island/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(n)/ou=RSS Diego Garcia(n)
ROLE	Sub-Registration Authority
PLA	SUBREGAUTH DG(n)
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Die go Garcia Island/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(n)/ou=RSS Diego Garcia(n)/ou=SUBREGAUTH DG(n)
ROLE	Certificate Authority
PLA	CERTAUTH0029 DG(n)
POC	IT1 Scott Leaf
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Die go Garcia Island/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(n)/ou=RSS Diego Garcia(n)/ou=CERTAUTH0029 DG(n)
ROLE	Help Desk
PLA	HELPDESK DG(n)

<b>NCTS Diego Garcia SBU DMS LNOSC OPERATIONS ROLES</b>	
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Diego Garcia Island/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(n)/ou=RSS Diego Garcia(n)/ou=HELPDESK DG(n)
ROLE	DMS Operations Manager
PLA	DMSOPSMNGR-DG(n)
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Diego Garcia Island/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(n)/ou=RSS Diego Garcia(n)/ou=DMSOPSMNGR-DG(n)
ROLE	Area System Manager
PLA	LSM DIEGO GARCIA DG(n)
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, Ap 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Diego Garcia Island/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(n)/ou=RSS Diego Garcia(n)/ou=LMS DIEGO GARCIA(n)
ROLE	Directory Administrator
PLA	Directory Manager DG(n)
POC	IT1 Duane A. Bauer

<b>NCTS Diego Garcia SBU DMS LNOSC OPERATIONS ROLES</b>	
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Diego Garcia Island/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(n)/ou=RSS Diego Garcia(n)/ou=DIRECTORY MANAGER DG(n)
ROLE	Mail List Manager
PLA	MLMANAGER DG(n)
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Diego Garcia Island/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(n)/ou=RSS Diego Garcia(n)/ou=MLMANAGER DG(n)
ROLE	Mail List Administrator
PLA	N/A
POC	N/A
ADDRESS	N/A
PHONE/FAX	Comm: N/A              FAX: N/A              DSN: N/A
E-MAIL	Please use X.500 address
X.500	N/A
ROLE	Configuration Manager
PLA	CONFIGMNGR DG(n)
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333

<b>NCTS Diego Garcia SBU DMS LNOSC OPERATIONS ROLES</b>	
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Diego Garcia Island/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(n)/ou=RSS Diego Garcia(n)/ou=CONFIGMNGR DG(n)
ROLE	Security Officer
PLA	SECURITY OFFICER DG(n)
POC	IT1 Scott Leaf
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations/l=Diego Garcia Island/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(n)/ou=RSS Diego Garcia(n)/ou=SECURITY-OFFICER DG(n)



<b>NCTS DIGEO GARCIA SIPR DMS LNOSC OPERATIONS ROLES</b>	
PLA	NAVCOMTELSTA DIEGO GARCIA
LNOSC TYPE	DMS RSS
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l= Diego Garcia Island(s)/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(s)/ou=RSS Diego Garcia(s)
ROLE	Sub-Registration Authority
PLA	SUBREGAUTH DG(s)
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l= Diego Garcia Island(s)/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(s)/ou=RSS Diego Garcia(s)/ou=SUBREGAUTH DG(s)
ROLE	Certificate Authority
PLA	CERTAUTH0029 DG(s)
POC	IT1 Scott Leaf
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l= Diego Garcia Island(s)/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(s)/ou=RSS Diego Garcia(s)/ou=CERTAUTH0029 DG(s)
ROLE	Help Desk

<b>NCTS DIGEO GARCIA SIPR DMS LNOSC OPERATIONS ROLES</b>	
PLA	HELPDESK DG(s)
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l= Diego Garcia Island(s)/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(s)/ou=RSS Diego Garcia(s)/ou=HELPDESK DG(s)
ROLE	DMS Operations Manager
PLA	DMSOPSMNGR-DG(s)
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l= Diego Garcia Island(s)/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(s)/ou=RSS Diego Garcia(s)/ou=DMSOPSMNGR-DG(s)
ROLE	Area System Manager
PLA	LSM DIEGO GARCIA DG(s)
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, Ap 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l= Diego Garcia Island(s)/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(s)/ou=RSS Diego Garcia(s)/ou=LMS DIEGO GARCIA(s)
ROLE	Directory Administrator
PLA	Directory Manager DG(s)

<b>NCTS DIGEO GARCIA SIPR DMS LNOSC OPERATIONS ROLES</b>	
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l= Diego Garcia Island(s)/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(s)/ou=RSS Diego Garcia(s)/ou=DIRECTORY MANAGER DG(s)
ROLE	Mail List Manager
PLA	MLMANAGER DG(s)
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l= Diego Garcia Island(s)/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(s)/ou=RSS Diego Garcia(s)/ou=MLMANAGER DG(s)
ROLE	Mail List Administrator
PLA	N/A
POC	N/A
ADDRESS	N/A
PHONE/FAX	Comm: N/A              FAX: N/A              DSN: N/A
E-MAIL	Please use X.500 address
X.500	N/A
ROLE	Configuration Manager
PLA	CONFIGMNGR DG(s)
POC	IT1 Duane A. Bauer
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008

<b>NCTS DIGEO GARCIA SIPR DMS LNOSC OPERATIONS ROLES</b>	
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l= Diego Garcia Island(s)/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(s)/ou=RSS Diego Garcia(s)/ou=CONFIGMNGR DG(s)
ROLE	Security Officer
PLA	SECURITY OFFICER DG(s)
POC	IT1 Scott Leaf
ADDRESS	NCTS DIEGO GARCIA PSC 466 BOX 8  FPO, AP 96595-0008
PHONE/FAX	Comm: 011-246-      FAX: DSN 315-      DSN: 315-370- 370-2333              370-2301              2333
E-MAIL	Please use X.500 address
X.500	/c=US/o=U.S. Government/ou=DoD/ou=Navy/ou=Organizations(s)/l= Diego Garcia Island(s)/l=DIEGO GARCIA/ou=NAVCOMTELSTA DIEGO GARCIA(s)/ou=RSS Diego Garcia(s)/ou=SECURITY-OFFICER DG(s)

NAVCOMTELSTA GUAM GU(N) DMS LNOSC OPERATIONS ROLES	
PLA	NAVCOMTELSTA GUAM GU
LNOSC TYPE	RSS
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-5961      FAX: 671-355-5310      DSN: 355-5961
E-MAIL	
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(n),l=GUAM,ou=NAVCOMTELSTA GUAM GU(n)
ROLE	Sub-Registration Authority
PLA	NAVCOMTELSTA GUAM GU (SRA NOT USED AT THIS COMMAND)
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-5026      FAX: 671-355-5310      DSN: 355-5026
E-MAIL	santanal@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(n),l=GUAM,ou=NAVCOMTELSTA GUAM GU(n),OU:RSS Guam(n),cn:SUBREGAUTH GUAM(n)
ROLE	Certificate Authority
PLA	NAVCOMTELSTA GUAM GU
POC	IT2 Richard Wade
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-5856      FAX: 671-355-5310      DSN: 355-5856
E-MAIL	wader@nctsguam@navy.mil

<b>NAVCOMTELSTA GUAM GU(N) DMS LNOSC OPERATIONS ROLES</b>	
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(n),l=GUAM,ou=NAVCOMTELSTA GUAM GU(n),OU:RSS Guam(n),cn:CERTAUTH1 GUAM(n)
ROLE	Help Desk
PLA	NAVCOMTELSTA GUAM GU
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BPX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355- 5026      FAX: 671-355- 5310      DSN: 355-5026
E-MAIL	IT1 LUISA SANTANA
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(n),l=GUAM,ou=NAVCOMTELSTA GUAM GU(n),OU:RSS Guam(n) OU:MS HELPDESK GUAM(n)
ROLE	DMS Operations Manager
PLA	NAVCOMTELSTA GUAM GU
POC	ITC(AW) CHERYL SEAY
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355- 5961      FAX: 671-355- 5310      DSN: 355-5961
E-MAIL	seayc@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(n),l=GUAM,ou=NAVCOMTELSTA GUAM GU(n),OU:RSS Guam(n) CN:DMSOPSMNGR GUAM(n)
ROLE	Area System Manager
PLA	NAVCOMTELSTA GUAM GU
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355- 5026      FAX: 671-355- 5310      DSN: 355-5026

<b>NAVCOMTELSTA GUAM GU(N) DMS LNOSC OPERATIONS ROLES</b>	
E-MAIL	santanal@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(n),l=GUAM,ou=NAVCOMTELSTA GUAM GU(n),OU:RSS Guam(n) CN:ASM GUAM(n)
ROLE	Directory Administrator
PLA	NAVCOMTELSTA GUAM GU
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355- 5026      FAX: 671-355- 5310      DSN: 355-5026
E-MAIL	santanal@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(n),l=GUAM,ou=NAVCOMTELSTA GUAM GU(n),OU:RSS Guam(n) CN:DIRADMIN1 GUAM(n)
ROLE	Mail List Manager
PLA	NAVCOMTELSTA GUAM GU
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355- 5026      FAX: 671-355- 5310      DSN: 355-5026
E-MAIL	santanal@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(n),l=GUAM,ou=NAVCOMTELSTA GUAM GU(n),OU:RSS Guam(n) CN:MLMANAGER GUAM(n)
ROLE	Mail List Administrator
PLA	NAVCOMTELSTA GUAM GU
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537

<b>NAVCOMTELSTA GUAM GU(N) DMS LNOSC OPERATIONS ROLES</b>	
PHONE/FAX	Comm: 671-355-5026      FAX: 671-355-5310      DSN: 355-5026
E-MAIL	santanal@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(n),l=GUAM,ou=NAVCOMTELSTA GUAM GU(n),OU:RSS Guam(n) CN:MLMANAGER GUAM(n)
ROLE	Configuration Manager
PLA	NAVCOMTELSTA GUAM GU
POC	ITC(AW) CHERYL SEAY
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-5961      FAX: 671-355-5310      DSN: 355-5961
E-MAIL	seayc@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(n),l=GUAM,ou=NAVCOMTELSTA GUAM GU(n),OU:RSS Guam(n) CN:CONFIGMNGR GUAM(n)
ROLE	Security Officer
PLA	NAVCOMTELSTA GUAM GU
POC	ITC(AW) CHERYL SEAY
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-5961      FAX: 671-355-5310      DSN: 355-5961
E-MAIL	seayc@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(n),l=GUAM,ou=NAVCOMTELSTA GUAM GU(n),OU:RSS Guam(n) CN:SECURITY-OFFICER GUAM(n)



NAVCOMTELSTA GUAM GU(S) DMS LNOSC OPERATIONS ROLES	
PLA	NAVCOMTELSTA GUAM GU
LNOSC TYPE	RSS
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-5961      FAX: 671-355-5310      DSN: 355-5961
E-MAIL	
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(s),l=GUAM,ou=NAVCOMTELSTA GUAM GU(s)
ROLE	Sub-Registration Authority
PLA	NAVCOMTELSTA GUAM GU (SRA NOT USED AT THIS COMMAND)
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-5026      FAX: 671-355-5310      DSN: 355-5026
E-MAIL	santanal@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(s),l=GUAM,ou=NAVCOMTELSTA GUAM GU(s),OU:RSS Guam(s),cn:SUBREGAUTH GUAM(s)
ROLE	Certificate Authority
PLA	NAVCOMTELSTA GUAM GU
POC	IT2 Richard Wade
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-5856      FAX: 671-355-5310      DSN: 355-5856
E-MAIL	wader@nctsguam@navy.mil

<b>NAVCOMTELSTA GUAM GU(S) DMS LNOSC OPERATIONS ROLES</b>	
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(s),l=GUAM,ou=NAVCOMTELSTA GUAM GU(s),OU:RSS Guam(s),cn:CERTAUTH1 GUAM(s)
ROLE	Help Desk
PLA	NAVCOMTELSTA GUAM GU
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BPX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355- 5026      FAX: 671-355- 5310      DSN: 355-5026
E-MAIL	IT1 LUISA SANTANA
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(s),l=GUAM,ou=NAVCOMTELSTA GUAM GU(s),OU:RSS Guam(s) OU:MS HELPDESK GUAM(s)
ROLE	DMS Operations Manager
PLA	NAVCOMTELSTA GUAM GU
POC	ITC(AW) CHERYL SEAY
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355- 5961      FAX: 671-355- 5310      DSN: 355-5961
E-MAIL	seayc@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(s),l=GUAM,ou=NAVCOMTELSTA GUAM GU(s),OU:RSS Guam(s) CN:DMSOPSMNGR GUAM(s)
ROLE	Area System Manager
PLA	NAVCOMTELSTA GUAM GU
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355- 5026      FAX: 671-355- 5310      DSN: 355-5026

<b>NAVCOMTELSTA GUAM GU(S) DMS LNOSC OPERATIONS ROLES</b>	
E-MAIL	santanal@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(s),l=GUAM,ou=NAVCOMTELSTA GUAM GU(s),OU:RSS Guam(s) CN:ASM GUAM(s)
ROLE	Directory Administrator
PLA	NAVCOMTELSTA GUAM GU
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-      FAX: 671-355-      DSN: 355-5026 5026                      5310
E-MAIL	santanal@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(s),l=GUAM,ou=NAVCOMTELSTA GUAM GU(s),OU:RSS Guam(s) CN:DIRADMIN1 GUAM(s)
ROLE	Mail List Manager
PLA	NAVCOMTELSTA GUAM GU
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-      FAX: 671-355-      DSN: 355-5026 5026                      5310
E-MAIL	santanal@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUA M(s),l=GUAM,ou=NAVCOMTELSTA GUAM GU(s),OU:RSS Guam(s) CN:MLMANAGER GUAM(s)
ROLE	Mail List Administrator
PLA	NAVCOMTELSTA GUAM GU
POC	IT1 LUISA SANTANA
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537

<b>NAVCOMTELSTA GUAM GU(S) DMS LNOSC OPERATIONS ROLES</b>	
PHONE/FAX	Comm: 671-355-5026      FAX: 671-355-5310      DSN: 355-5026
E-MAIL	santanal@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUAM(s),l=GUAM,ou=NAVCOMTELSTA GUAM GU(s),OU:RSS Guam(s) CN:MLMANAGER GUAM(s)
ROLE	Configuration Manager
PLA	NAVCOMTELSTA GUAM GU
POC	ITC(AW) CHERYL SEAY
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-5961      FAX: 671-355-5310      DSN: 355-5961
E-MAIL	seayc@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUAM(s),l=GUAM,ou=NAVCOMTELSTA GUAM GU(s),OU:RSS Guam(s) CN:CONFIGMNGR GUAM(s)
ROLE	Security Officer
PLA	NAVCOMTELSTA GUAM GU
POC	ITC(AW) CHERYL SEAY
ADDRESS	NAVCOMTELSTA GUAM PSC 488 BOX 101 FPO AP 96537
PHONE/FAX	Comm: 671-355-5961      FAX: 671-355-5310      DSN: 355-5961
E-MAIL	seayc@nctsguam.navy.mil
X.500	c=US;o=U.S. Government;ou=DoD;ou=NAVY;ou=Organizations;l=GUAM(s),l=GUAM,ou=NAVCOMTELSTA GUAM GU(s),OU:RSS Guam(s) CN:SECURITY-OFFICER GUAM(s)

NCTAMS LANT DET HAMPTON ROADS NORFOLK VA(N) DMS LNOSC OPERATIONS ROLES	
PLA	NCTAMS LANT DET HAMPTON ROADS NORFOLK VA(N)
LNOSC TYPE	RSS Hampton Roads Norfolk VA(n)
ADDRESS	7927 Ingersol ST STE 300 NH-95  Norfolk, VA 23551-2398
PHONE/FAX	Comm: (757)                      FAX: (757)                      DSN: 836-0691 836-0691                      836-5627
E-MAIL	@dmslant.navy.mil
X.500	ou=NCTAMS LANT DET HAMPTON ROADS NORFOLK VA(n),ou=RSS Hampton roads Norfolk VA(n)
ROLE	Sub-Registration Authority
PLA	SUBREGAUTH Hampton Roads Norfolk(n)
POC	IT2 Micheal B. Jennings
ADDRESS	7927 Ingersol ST STE 300 NH-95  Norfolk, VA 23551-2398
PHONE/FAX	Comm: (757)                      FAX: (757)                      DSN: 836-0691 836-0691                      836-5627
E-MAIL	@dmslant.navy.mil
X.500	ou=RSS Hampton Roads Norfolk VA(n),cn=SUBREGAUTH Hampton Roads Norfolk(n)
ROLE	Certificate Authority
PLA	CERTAUTH0043 (U-NCTAMS LANT Det Hampton Roads VA)
POC	Edward Brown
ADDRESS	7927 Ingersol ST STE 300 NH-95  Norfolk, VA 23551-2398
PHONE/FAX	Comm: (757)                      FAX: (757)                      DSN: 836-7969 836-7969                      836-5627
E-MAIL	@dmslant.navy.mil
X.500	c=US,o=U.S. Government,ou=DoD,ou=Navy,cn=CERTAUTH0043 [U- NCTAMS LANT Det Hampton Roads Norfolk VA]
ROLE	Help Desk
PLA	HELPDESK Hampton Roads Norfolk(n)
POC	Karla Campbell

NCTAMS LANT DET HAMPTON ROADS NORFOLK VA(N) DMS LNOSC OPERATIONS ROLES	
ADDRESS	7927 Ingersol ST STE 300 NH-95  Norfolk, VA 23551-2398
PHONE/FAX	Comm: (757)                      FAX: (757)                      DSN: 836-0691 836-0691                      836-5627
E-MAIL	@dmslant.navy.mil
X.500	ou=RSS Hampton Roads Norfolk VA(n),cn=HELPDESK Hampton Roads Norfolk(n)
ROLE	DMS Operations Manager
PLA	DMSOPSMNGR Hampton Roads Norfolk(n)
POC	Peter J. Gordon
ADDRESS	7927 Ingersol ST STE 300 NH-95  Norfolk, VA 23551-2398
PHONE/FAX	Comm: (757)                      FAX: (757)                      DSN: 836-7561 836-7561                      836-5627
E-MAIL	@dmslant.navy.mil
X.500	ou=RSS Hampton Roads Norfolk VA(n),cn=DMSOPSMNGR Hampton Roads Norfolk(n)
ROLE	Area System Manager
PLA	LSM Hampton Roads Norfolk(n)
POC	Peter J. Gordon
ADDRESS	7927 Ingersol ST STE 300 NH-95  Norfolk, VA 23551-2398
PHONE/FAX	Comm: (757)                      FAX: (757)                      DSN: 836-7561 836-7561                      836-5627
E-MAIL	@dmslant.navy.mil
X.500	ou=RSS Hampton Roads Norfolk VA(n),cn=LSM Hampton Roads Norfolk(n)
ROLE	Directory Administrator
PLA	Directory Manager HRVA(n)
POC	IT2 Micheal B. Jennings
ADDRESS	7927 Ingersol ST STE 300 NH-95  Norfolk, VA 23551-2398
PHONE/FAX	Comm: (757)                      FAX: (757)                      DSN: 836-0691 836-0691                      836-5627
E-MAIL	@dmslant.navy.mil
X.500	ou=RSS Hampton Roads Norfolk VA(n),cn=Directory Manager HRVA(n)
ROLE	Mail List Manager

NCTAMS LANT DET HAMPTON ROADS NORFOLK VA(N) DMS LNOSC OPERATIONS ROLES	
PLA	MLMANAGER Hampton Roads Norfolk(n)
POC	IT2 Micheal B. Jennings
ADDRESS	7927 Ingersol ST STE 300 NH-95  Norfolk, VA 23551-2398
PHONE/FAX	Comm: (757)                      FAX: (757)                      DSN: 836-0691 836-0691                      836-5627
E-MAIL	@dmslant.navy.mil
X.500	ou=RSS Hampton Roads Norfolk VA(n),cn=MLMANAGER Hampton Roads Norfolk(n)
ROLE	Mail List Administrator
PLA	MLADMIN-1 Hampton Roads Norfolk(n)
POC	Karla Campbell
ADDRESS	7927 Ingersol ST STE 300 NH-95  Norfolk, VA 23551-2398
PHONE/FAX	Comm: (757)                      FAX: (757)                      DSN: 836-0691 836-0691                      836-5627
E-MAIL	@dmslant.navy.mil
X.500	ou=RSS Hampton Roads Norfolk VA(n),cn=MLADMIN-1 Hampton Roads Norfolk(n)
ROLE	Configuration Manager
PLA	CONFIGMNGR Hampton Roads Norfolk(n)
POC	Karla Campbell
ADDRESS	7927 Ingersol ST STE 300 NH-95  Norfolk, VA 23551-2398
PHONE/FAX	Comm: (757)                      FAX: (757)                      DSN: 836-0691 836-0691                      836-5627
E-MAIL	@dmslant.navy.mil
X.500	ou=RSS Hampton Roads Norfolk VA(n),cn=CONFIGMNGR Hampton Roads Norfolk(n)
ROLE	Security Officer
PLA	SECURITY OFFICER Hampton Roads Norfolk(n)
POC	Peter J. Gordon
ADDRESS	7927 Ingersol ST STE 300 NH-95  Norfolk, VA 23551-2398
PHONE/FAX	Comm: (757)                      FAX: (757)                      DSN: 836-7561 836-7561                      836-5627
E-MAIL	@dmslant.navy.mil

<b>NCTAMS LANT DET HAMPTON ROADS NORFOLK VA(N)</b>	
<b>DMS LNOSC OPERATIONS ROLES</b>	
X.500	ou=RSS Hampton Roads Norfolk VA(n),cn=SECURITY OFFICER Hampton Roads Norfolk(n)



DMS LNOSC OPERATIONS ROLES	
PLA	NAVCOMTELSTA PENSACOLA FL
LNOSC TYPE	RSS
ADDRESS	130 WEST AVENUE SUITE B PENSACOLA FL NAVCOMTELSTA N31 32508-5111,
PHONE/FAX	Comm: 850-452-      FAX: 850-452-      DSN: 922-7957 7957                      9106
E-MAIL	
X.500	C=US/O=U.S.Government/OU=DoD/OU=NAVY/OU=Organiza tions/L=Florida/L=PENSACOLA/OU=NAVCOMTESLTA PENSACOLA FL(n)/OU=RSS Pensacola Fl(n)
ROLE	Sub-Registration Authority
PLA	
POC	HENRY L. BLACK
ADDRESS	130 WEST AVENUE SUITE B PENSACOLA FL NAVCOMTELSTA N31 32508-5111,
PHONE/FAX	Comm: 850-452-      FAX: 850-452-      DSN: 922-7952 7952                      9106
E-MAIL	BLACKH@NCTSPENS.NAVY.MIL
X.500	C=US/O=U.S.Government/OU=DoD/OU=NAVY/OU=Organiza tions/L=Florida/L=PENSACOLA/OU=NAVCOMTESLTA PENSACOLA FL(n)/OU=RSS Pensacola Fl(n)/CN=SUBREGAUTH Pensacola(n)
ROLE	Certificate Authority
PLA	
POC	DARL W. MELLON
ADDRESS	130 WEST AVENUE SUITE B PENSACOLA FL NAVCOMTELSTA N31 32508-5111,
PHONE/FAX	Comm: 850-452-      FAX: 850-452-      DSN: 922-7966 7966                      9106
E-MAIL	MELLOND@NCTSPENS.NAVY.MIL
X.500	C=US/O=U.S.Government/OU=DoD/OU=NAVY/OU=Organiza tions/L=Florida/L=PENSACOLA/OU=NAVCOMTESLTA PENSACOLA FL(n)/OU=RSS Pensacola Fl(n)/CN=CERTAUTH Pensacola(n)
ROLE	Help Desk
PLA	
POC	HELLEM SPENCER

DMS LNOSC OPERATIONS ROLES	
ADDRESS	130 WEST AVEUNE SUITE B NAVCOMTELSTA N31 PENSACOLA FL 32508-5111,
PHONE/FAX	Comm: (850)                      FAX: (850)                      DSN: 922-3621 452-3621                              452-9106
E-MAIL	SPENCERH@NCTS.NAVY.MIL
X.500	C=US/O=U.S.Government/OU=DoD/OU=NAVY/OU=Organiza tions/L=Florida/L=PENSACOLA/OU=NAVCOMTESLTA PENSACOLA FL(n)/OU=RSS Pensacola Fl(n)/CN=HELPPDESK Pensacola(n)
ROLE	DMS Operations Manager
PLA	
POC	HUBERT COBBS
ADDRESS	130 WEST AVENUE SUITE B NAVCOMTELSTA N31 PENSACOLA FL 32508-5111,
PHONE/FAX	Comm: 850-452-                      FAX: 850-452-                      DSN: 922-7957 7957                                      9106
E-MAIL	COBBSR@NCTSPENS.NAVY.MIL
X.500	C=US/O=U.S.Government/OU=DoD/OU=NAVY/OU=Organiza tions/L=Florida/L=PENSACOLA/OU=NAVCOMTESLTA PENSACOLA FL(n)/OU=RSS Pensacola Fl(n)/CN=DMSOPSMNGR Pensacola(n)
ROLE	Area System Manager
PLA	
POC	
ADDRESS	
PHONE/FAX	Comm:                                      FAX:                                      DSN:
E-MAIL	
X.500	
ROLE	Directory Administrator
PLA	
POC	
ADDRESS	
PHONE/FAX	Comm:                                      FAX:                                      DSN:
E-MAIL	
X.500	
ROLE	Mail List Manager
PLA	

DMS LNOSC OPERATIONS ROLES	
POC	IT2 ROCHELLE BOLTON
ADDRESS	130 WEST AVENUE SUITE B NAVCOMTELSTA N31 PENSACOLA FL 32508-5111,
PHONE/FAX	Comm: 850-452-      FAX: 850-452-      DSN: 922-3621 3621                      9106
E-MAIL	BOLTONR@NCTS.NAVY.MIL
X.500	C=US/O=U.S.Government/OU=DoD/OU=NAVY/OU=Organiza tions/L=Florida/L=PENSACOLA/OU=NAVCOMTESLTA PENSACOLA FL(n)/OU=RSS Pensacola Fl(n)/CN=MLMANAGER Pensacola(n)
ROLE	Mail List Administrator
PLA	
POC	
ADDRESS	
PHONE/FAX	Comm:                      FAX:                      DSN:
E-MAIL	
X.500	
ROLE	Configuration Manager
PLA	
POC	IT1 YOLANDA POLK
ADDRESS	130 WEST AVENUE SUITE B NAVCOMTELSTA N31 PENSACOLA FL 32508-5111,
PHONE/FAX	Comm: 850-452-      FAX: 850-452-      DSN: 922-3621 3621                      9106
E-MAIL	POLKY@NCTSPENS.NAVY.MIL
X.500	C=US/O=U.S.Government/OU=DoD/OU=NAVY/OU=Organiza tions/L=Florida/L=PENSACOLA/OU=NAVCOMTESLTA PENSACOLA FL(n)/OU=RSS Pensacola Fl(n)/CN=CONFIGMNGR Pensacola(n)
ROLE	Security Officer
PLA	
POC	CYNTHIA SANTOS
ADDRESS	130 WEST AVENUE SUITE B NAVCOMTELSTA N31 PENSACOLA FL 32508-5111,
PHONE/FAX	Comm: 850-452-      FAX: 850-452-      DSN: 922-7969 7969                      9106
E-MAIL	SANTOSC@NCTSPENS.NAVY.MIL

<b>DMS LNOSC OPERATIONS ROLES</b>	
X.500	C=US/O=U.S.Government/OU=DoD/OU=NAVY/OU=Organizations/L=Florida/L=PENSACOLA/OU=NAVCOMTESLTA PENSACOLA FL(n)/OU=RSS Pensacola Fl(n)/CN=SECURITY OFFICER Pensacola(n)
ROLE	Local Service Manager
PLA	
POC	IT1 YOLANDA POLK
ADDRESS	130 WEST AVENUE SUITE B NAVCOMTELSTA N31 PENSACOLA FL 32508-5111,
PHONE/FAX	Comm: 850-452-      FAX: 850-452-      DSN: 922-7969 3621                      9106
E-MAIL	POLKY@NCTSPENS.NAVY.MIL
X.500	C=US/O=U.S.Government/OU=DoD/OU=NAVY/OU=Organizations/L=Florida/L=PENSACOLA/OU=NAVCOMTESLTA PENSACOLA FL(n)/OU=RSS Pensacola Fl(n)/CN=LSM Pensacola(n)

APPENDIX D

DMS MANAGEMENT OPERATIONAL ACCOUNTS

**DMS MANAGEMENT OPERATIONAL ACCOUNTS****D1. NIPRNET ACCOUNTS****GSM**

C=US/O=U.S.Government/OU=DoD/DISA/OU=Organizations/OU=GOSC/OU=ORG STAFF/OU=OPS/CN=DMS GSM

**RNOSC-CONUS**

C=US/O=U.S.Government/OU=DoD/OU=DISA/OU=Organizations/OU=GOSC/OU=RNOSC-Columbus/CN=Controller

**RNOSC-EUROPE**

C=US/O=U.S.Government/OU=DoD/OU=DISA/OU=Organizations/OU=GOSC/OU=RNOSC-Europe/CN=OPS DIR

**RNOSC-PACIFIC**

C=US/O=U.S.Government/OU=DISA/OU=Organizations/OU=GOSC/OU=RNOSC-Pacific/CN=RNOSC-P1

**D2. SIPRNET ACCOUNTS****GSM**

C=US/O=U.S.Government/OU=DoD/OU=DISA/OU=Organizations/OU=GOSC/OU=ORG STAFF(s)/OU=OPS/CN=DMS GSM(s)

**RNOSC-CONUS**

C=US/O=U.S.Government/OU=DoD/OU=DISA/OU=Organizations/OU=GOSC/OU=RNOSC-Columbus/CN=ITAC01

**RNOSC-EUROPE**

C=US/O=U.S.Government/OU=DoD/OU=DISA/OU=Organizations/OU=GOSC/OU=RNOSC-Europe/CN=OPS DIR(s)

**RNOSC-PACIFIC**

C=US/O=U.S.Government/OU=DoD/OU=DISA/OU=Organizations/OU=GOSC/OU=RNOSC-Pacific/CN=RNOSC-P2(s)

**D3. SECRET RNOSC ACCOUNTS****DTH-CONUS**

C=US/O=U.S.Government/OU=DoD/OU=AUTODIN PLAs/OU=DTH Services/OU=CONUS DTH(t)/OU=DTH Operations Director(t)

**DTH-EUROPE**

C=US/O=U.S.Government/OU=DoD/OU=AUTODIN PLAs/OU=DTH Services/OU=EUROPE DTH(t)/OU=DTH Operations Director(t)

**DTH-PACIFIC**

C=US/O=U.S.Government/OU=DoD/OU=AUTODIN PLAs/OU=DTH Services/OU=Pacific DTH(t)/OU=DTH Operations Director(t)