



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**THE DEFENSE MESSAGING SYSTEM (DMS) IN THE NAVY
REGIONAL ENTERPRISE MESSAGING SYSTEM (NREMS)
ENVIRONMENT: EVIDENCE THAT SIZE DOES MATTER IN
DOD BUSINESS PROCESS ENGINEERING**

by

Alice Y. Liburd
Avonna S. Ramsey

June 2007

Thesis Advisor:
Co-Advisor:

Karl Pfeiffer
Philip Candreva

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June 2007	3. REPORT TYPE AND DATES COVERED Master's Thesis
4. TITLE AND SUBTITLE The Defense Messaging System (DMS) in the Navy Regional Enterprise Messaging System (NREMS) Environment: Evidence that Size Does Matter in DoD Business Process Engineering		5. FUNDING NUMBERS	
6. AUTHOR(S) Liburd, Alice Y. and Ramsey, Avonna S.		8. PERFORMING ORGANIZATION REPORT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) PEO C4I PMW 160.3 Naval Messaging		11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.	
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) Since the migration of DOD messaging to the DMS has been mandated, implementation has been less than ideal and otherwise unsuccessful. DMS users have reported dissatisfaction with the systems maintenance and security support burdens in the current client-server model. NREMS introduces a networked environment capable of push technology and centralized database and security management which should significantly reduce the DMS shortfalls that have made the system lack appeal to the end user. As the DOD seeks to solve these issues, other potential issues are introduced that must be reviewed and addressed to ensure a successful implementation of the NREMS. The Architecture Trade-off Analysis Method (ATAM) and user surveys formed the basis for analysis, conclusions, and recommendations. The goal of the ATAM is to understand the consequences of architectural decisions with respect to the quality attribute requirements of the system. User surveys provided the data to characterize the current naval messaging business process for each naval command and across the Navy with the prospect of properly defining future NREMS users. Combined analysis provided a clear understanding of the alternative architecture to the existing DMS architecture.			
14. SUBJECT TERMS DMS, NREMS, Messaging, BPR, Defense Message System, Navy Regional Message System, Business Process Reengineering			15. NUMBER OF PAGES 159
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**THE DEFENSE MESSAGING SYSTEM (DMS) IN THE NAVY REGIONAL
ENTERPRISE MESSAGING SYSTEM (NREMS) ENVIRONMENT: EVIDENCE
THAT SIZE DOES MATTER IN DOD BUSINESS PROCESS ENGINEERING**

Alice Y. Liburd
Lieutenant, United States Navy
B.S., Texas A & M University, 1998
MBA, Southern New Hampshire University, 2002

Avonna S. Ramsey
Lieutenant Commander, United States Navy
B.S., University of Oklahoma, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
June 2007**

Author: Alice Y. Liburd

Avonna S. Ramsey

Approved by: Karl Pfeiffer, Ph.D., LtCol USAF
Thesis Advisor

Philip Candreva
Co-Advisor

Dan Boger, Ph.D.
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Since the migration of DOD messaging to the DMS has been mandated, implementation has been less than ideal and otherwise unsuccessful. DMS users have reported dissatisfaction with the systems maintenance and security support burdens in the current client-server model. NREMS introduces a networked environment capable of push technology and centralized database and security management which should significantly reduce the DMS shortfalls that have made the system lack appeal to the end user. As the DOD seeks to solve these issues, other potential issues are introduced that must be reviewed and addressed to ensure a successful implementation of the NREMS.

The Architecture Trade-off Analysis Method (ATAM) and user surveys formed the basis for analysis, conclusions, and recommendations. The goal of the ATAM is to understand the consequences of architectural decisions with respect to the quality attribute requirements of the system. User surveys provided the data to characterize the current naval messaging business process for each naval command and across the Navy with the prospect of properly defining future NREMS users. Combined analysis provided a clear understanding of the alternative architecture to the existing DMS architecture.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION	1
A.	OBJECTIVES	2
B.	SCOPE	3
C.	ORGANIZATION	3
II.	BACKGROUND	5
A.	NREMS GENESIS	5
1.	Commander, Fleet Forces Command (COMFLTFORCOM)	5
2.	Naval Messaging Working Group	8
B.	NREMS PROJECT	10
1.	Goal	10
2.	Features	10
a.	<i>Site and Manpower Reduction</i>	11
b.	<i>Consistent with Net-Centric Enterprise Services (NCES) Strategy</i>	11
c.	<i>Joint DMS Core Product</i>	12
d.	<i>Single Message Store at a Regional Node</i>	12
e.	<i>Common Business Practices</i>	13
C.	CURRENT STATUS OF NREMS	13
D.	FUTURE STATE OF NREMS	16
III.	CHANGE MANAGEMENT FOR DOD COMMUNICATION SYSTEMS	17
A.	CATALYST FOR CHANGE	17
B.	ROLES OF CHANGE PARTICIPANTS	20
C.	AN ANALYSIS OF THE NREMS PROJECT CHANGE MANAGEMENT APPROACH	22
1.	The Ten Commandments of Implementing Change	22
a.	<i>Analyze the Organization and its Need for Change</i>	23
b.	<i>Create a Shared Vision and Common Direction</i>	23
c.	<i>Separate from the Past</i>	23
d.	<i>Create a Sense of Urgency</i>	23
e.	<i>Support a Strong Leader Role</i>	24
f.	<i>Line Up Political Sponsorship</i>	24
g.	<i>Craft an Implementation Plan</i>	24
h.	<i>Develop Enabling Structures</i>	24
i.	<i>Communicate, Involve People, and Be Honest</i>	25
j.	<i>Reinforce and Institutionalize Change</i>	25
2.	Analysis	25
D.	CONCLUSION	32

IV.	REVIEW OF NAVAL MESSAGING ARCHITECTURE	35
A.	DEFENSE MESSAGING SYSTEM (DMS)	35
1.	Strategic Concept	36
2.	Operational Requirements	37
3.	Problem Characterization	38
a.	DMS Client Maintenance	39
b.	FORTEZZA Logistics	39
4.	Analysis of Architectural Guidance	39
B.	NAVY REGIONAL ENTERPRISE MESSAGING SYSTEM (NREMS)	40
1.	Strategic Concept	40
2.	Operational Requirements	41
3.	Problem Characterization	42
a.	NMCI Connectivity	43
b.	DOD PKI Availability	43
c.	Multi-user Capability	43
d.	CP-XP Service Restart Time	43
4.	Analysis of Architectural Guidance	44
V.	RESEARCH METHODOLOGY	47
A.	ARCHITECTURE TRADE-OFF ANALYSIS METHOD (ATAM)	48
B.	USER SURVEYS	49
VI.	RESEARCH ANALYSIS	53
A.	DMS ARCHITECTURE ANALYSIS	53
1.	Message Handling Services (MHS)	54
2.	Directory Services (DS)	54
3.	Security Services (SS)	54
4.	Interoperability Services (IS)	54
B.	NREMS ARCHITECTURE ANALYSIS	56
1.	CommPower CP-XP	57
2.	Telos AMHS	57
C.	QUALITY ATTRIBUTES	58
1.	Security	60
2.	Modeling Quality Attributes	64
3.	Maintainability/Supportability	70
D.	SCENARIOS	72
1.	Scenario 1: Failover	72
2.	Scenario 2: AMHS Server Quantity Variation ..	73
3.	Scenario 3: Peace Time vs. Wartime Surge	75
4.	Scenario 4: Wartime Surge and Failover	76
E.	USER SURVEYS	77
1.	NREMS Business Processes	78
2.	The Survey	79
a.	Survey Terminology	79
b.	Survey Development	81
c.	Survey Dissemination	81

3.	User Survey Analysis	82
a.	<i>Data Gathering</i>	83
b.	<i>Data Analysis</i>	84
c.	<i>Data Provided</i>	86
VII.	CONCLUSIONS	87
A.	ARCHITECTURE FEASIBILITY	87
1.	Interoperability	87
2.	Availability	88
a.	<i>Navy Marine Corps Intranet (NMCI)</i> <i>Connectivity</i>	88
b.	<i>DOD PKI availability</i>	89
c.	<i>CP-XP Service Restart Time</i>	89
3.	Scalability	90
a.	<i>Failover</i>	90
b.	<i>AMHS Server Quantity Increase</i>	90
4.	Maintainability	91
5.	Summary	92
B.	BUSINESS PROCESS REENGINEERING FEASIBILITY	93
1.	Change Management Analysis	93
2.	User Surveys	93
C.	SUMMARY OF CONCLUSIONS	95
1.	Architectural Transition Research	95
2.	Business Process Transition Research	96
a.	<i>The Transition Plan</i>	97
b.	<i>Business Processes</i>	98
3.	Summary	98
VIII.	RECOMMENDATIONS	101
A.	FINDINGS	101
B.	RECOMMENDATIONS FOR FUTURE STUDY	102
APPENDIX A.	SURVEY QUESTIONNAIRE	105
APPENDIX B.	SURVEY RESPONDENT DATA	111
APPENDIX C.	SURVEYMONKEY.COM SUMMARY REPORT	117
APPENDIX D.	SQL QUERIES DEVELOPED IN MICROSOFT ACCESS	123
APPENDIX E.	REPORTS GENERATED IN MICROSOFT ACCESS FOR EACH BUSINESS PROCESS	127
LIST OF REFERENCES		137
INITIAL DISTRIBUTION LIST		141

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	NREMS Implementation Schedule.....	15
Figure 2.	Naval Messaging Survey email disseminated to all registered NREMS users.....	51
Figure 3.	Naval Messaging Business Process Decision Tree (From: SAIC-PEO C4I PMW 160.3).....	52
Figure 4.	DMS Architecture (Functional View).....	56
Figure 5.	NREMS Architecture (Operational View) (From: PEO C4I 2005).....	58
Figure 6.	End User Web Access (NIPR) (From: PEO C4I 2007).	63
Figure 7.	End User Web Access (SIPR) (From: PEO C4I 2007).	63
Figure 8.	Arena Network Components Model (From: PEO C4I 2005).....	65
Figure 9.	Arena NCTAMS PAC Model (From: PEO C4I 2005).....	68
Figure 10.	NREMS High Level COOP Diagram (From: PEO C4I 2007).....	69
Figure 11.	NREMS Logical Diagram (From: PEO C4I 2007).....	70
Figure 12.	DMS Field Engineering Notification (FEN) (From: Email: TSA 2007).....	71
Figure 13.	Scenario 1 Failover Total Time in System.....	73
Figure 14.	Scenario 2 AMHS Server Quantity Variation.....	75
Figure 15.	Scenario 3 Peacetime vs Wartime Surge Total Time in System.....	75
Figure 16.	Scenario 4 Wartime Failover Total Time in System.....	76
Figure 17.	Naval Messaging Rush Hours.....	95

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	DMS Multicommand Required Operational Capability (MROC) 3-88 Requirements.....	19
Table 2.	OSI Reference Model Organization Matrix (CC4221 Notes 2002).....	64
Table 3.	Summary of Data from User Surveys.....	85
Table 4.	User Survey Statistics.....	94

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank Lieutenant Colonel Karl Pfeifer and Mr. Philip Candreva, for their patience and constant guidance during this research.

SPAWARSYSCEN San Diego experts offered excellent guidance, recommendations and advice during the information gathering and evaluation process phases.

LT Liburd would like to give a special thanks to her children son, Aaron and daughter, Taciana for remaining her biggest fans, as she pursues her career in the Navy and completes her many educational goals. Living with a single, ambitious, and daring mother has been no easy task and you both remain at the forefront of her mind as she moves forward in her career. She asks that you both remember that you are still her greatest accomplishments in life.

LCDR Ramsey would like to thank her family for their support throughout this endeavor. Her five year old son, Gabriel, always made the hardest academic day better with just a giggle and a smile. Her sister, Linda, saved her on many occasions by caring for Gabriel when studies became overwhelming. Her father and his wife, Roger and Ann, provided immeasurable help with their support, love and especially insight. Finally, she'd like to remember her mother, Masako, who passed away during her studies. She would not have come this far without her mother's tremendous example. To all of you, my love and gratitude.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

This thesis will focus on the Defense Messaging System (DMS) and its integration into the Navy Regional Enterprise Messaging System (NREMS). The transition from DMS to NREMS will occur at the same time as the transition from the Automatic Digital Network (AUTODIN) to DMS is completed.

Much anecdotal evidence exists to support end users' perception that the transition from AUTODIN to DMS was extremely difficult. The services did not have the infrastructure required to implement DMS, i.e., a sufficient local area network to support message traffic, FORTEZZA cards, or the Personal Computer Memory Card International Association (PCMCIA) cards. These costs were to be funded by local activities with limited budgets or understanding of DMS and its requirements. Initially, message service was slow at best and users were reluctant to transition from AUTODIN for fear of not receiving critical messages. In many cases, AUTODIN continues to operate, with DMS still not fully implemented.

The legacy of the transition from AUTODIN to NREMS is a tremendous amount of user distrust and reluctance to change, again, to a different system when AUTODIN hasn't been completely phased out, and NREMS has yet to be fully implemented. The purpose of this thesis is to articulate to the NREMS end user the following questions and responses with supporting research and analysis:

- Why the transition from DMS to NREMS? NREMS is a more cost effective solution requiring fewer resources than DMS that fulfills the requirements of Naval messaging.

- How will the transition be accomplished? Six defined business processes have been designed to support different Naval messaging organizational requirements. A decision tree will be provided to assist Naval messaging organizations in determining which business process best fits their messaging needs.

A. OBJECTIVES

This thesis will focus on the functional contribution and change management of the NREMS program implementation into the Navy. The NREMS architecture will be evaluated in a standardized manner utilizing the Architecture Trade-off Analysis Method (ATAM). The NREMS program implementation will be evaluated utilizing Todd Jick's (noted Harvard Business School change strategist) Ten Commandments of Implementing Change. Finally, Naval messaging user surveys will be used to characterize each Naval messaging organization's business process once transitioned to NREMS. To help reach this objective, the following supporting research questions were explored:

- How does the Classic DMS to NREMS architecture change contribute to: (1) the CNO direction for consolidation of communications resources on home soil, and (2) the CNO direction to transition off of and close down legacy systems?
 - What is the current Classic client server DMS architecture and where is it deployed?
 - What is the current NREMS architecture, its technical advantages, and where will it be deployed?
 - How does the NREMS implementation answer the CNO's direction and what are the key benefits in cost and performance?
- Evaluate the transition from DMS to NREMS.
 - Is the transition plan from DMS to NREMS effective? What are its strengths and weaknesses?

- Determine Naval messaging organizations' business process. How can commands be differentiated to support appropriate levels of service in order to create the appropriate requirements document for contract awarded to support NREMS?

B. SCOPE

The purpose of this thesis is to:

- Analyze the current and proposed naval messaging architectures and determine if NREMS will support Navy messaging requirements.
- Analyze the transition plan to determine its strengths and weaknesses.
- Provide a database, preformatted queries and preformatted reports that characterize Naval messaging business processes.

This research will not:

- Propose specific change actions for the implementation plan which is well underway.
- Provide recommended training programs as they have already been developed.

C. ORGANIZATION

Chapter II provides background material regarding the change requirement for Naval messaging.

Chapter III provides an analysis of the NREMS transition plan from a change management perspective.

Chapter IV presents a review of both Naval messaging architectures, DMS and NREMS.

Chapter V presents the research methodology used for the analysis of the architecture and the development of appropriate business processes.

Chapter VI presents is devoted to analysis: architecture and business processes.

Chapter VII provides the thesis conclusions.

Chapter VIII provides recommendations.

II. BACKGROUND

The Department of Defense's (DOD) Defense Message System (DMS) was developed as a replacement for DOD's antiquated AUTODIN system and was mandated as the messaging solution of choice for DOD in 1989. It is also cited as the solution for the Global Command and Control System (GCCS) Infrastructure Messaging Requirement. In October 2003, the Navy mandated a "Navy Enterprise DMS Messaging Solution."¹ In this chapter, we will discuss the history of the Navy's change requirement from the DMS client-server architecture to the Navy Regional Enterprise Messaging System (NREMS).

A. NREMS GENESIS

The requirement for NREMS began when the Commander, Fleet Forces Command recognized that the Navy's implementation of DMS did not support all of the Navy's needs for Naval Messaging. The Commander, Fleet Forces Command tasked the Naval Network Warfare Command with developing the future of Naval messaging. The Naval Network Warfare Command created the Naval Messaging Working Group, staffed with Naval messaging stakeholders, to manage the transition to the future Naval messaging system.

1. Commander, Fleet Forces Command (COMFLTFORCOM)

The Commander, Fleet Forces Command issued a message in October 2003 to outline a requirement for a standard Navy Enterprise DMS messaging solution to provide automated messaging and handling services for commands in both the

¹ Cited from the Commander, Fleet Forces Command Message dated 14 October 2003.

continental United States and outside of the continental United States commands. The Commander, Fleet Forces Command requested a solution that would address:

- Complex profiling
- Storage/retrospective search of archived messages
- Messaging utilities
- Servicing of non-delivery notices

The Commander, Fleet Forces Command also believed this to be the ideal opportunity to resolve existing installation, operations and maintenance issues related to the transition from AUTODIN to DMS which had not been entirely successful. These issues would be addressed by eliminating client software through the use of a web-enabled messaging portal, consolidating FORTEZZA cards at the regional messaging centers, and consolidating Navy DMS Messaging and IT experts at the regional sites where the assets would now be located.

Currently, Naval messaging assets are inconsistently maintained and manned depending on the expertise and resources available to individual commands. Software updates for client software are inconsistently applied and hardware suites are not consistently configured or maintained making it extremely difficult to address the multitude of issues that may arise. Commands would configure their DMS software and hardware to meet local needs and minimally address interoperability issues within Naval messaging. NREMS was commissioned to solve these issues.

The end state will move complex messaging tasks from non-IT personnel to messaging professionals, and will allow a reduction in the number of local control centers and regional server sites ... (thereby presenting) an opportunity to mitigate DMS installation, operations and maintenance issues, and improve governance, performance, security and cost.²

The evaluation criteria for the messaging requirement had to meet the following:

- Governance. The structure and policies of the solution would apply to all potential regional messaging centers with an emphasis on the standardization of delivery structures.
- Performance. Performance standards would be established that would mitigate lengthy down-times for Naval messaging.
- Security. Special handling for different categories of messages (classified vs. unclassified) with an emphasis on security clearance and control of access to messages.
- Cost. The solution must be evaluated using a cost/performance comparison model. The solution set should include government owned/government operated, government owned/contractor operated, contractor owned/contractor operated and any potential solutions offered by the NMCI contract.

The Commander, Fleet Forces Command requested that the Naval Network Warfare Command (NETWARCOM) develop the details and options. The Naval Network Warfare Command established the Naval Messaging Working Group (NMWG) to address the issues set forth by the Commander, Fleet Forces Command. The NMWG members have included Space and Naval Warfare Systems Command (U.S. Navy); the Naval Network Warfare Command; the Commander, Pacific Fleet; Naval Computer and Telecommunications Area Master Station, Atlantic; Naval Computer and Telecommunications Area

² Cited from the Commander, Fleet Forces Command Message dated 14 October 2003.

Master Station, Pacific; Office of the Chief of Naval Operations; and contractors Mitre and Booz Allen Hamilton.

In December 2003, the NMWG quickly recommended that the DISA approved Automated Message Handling System (AMHS) will be the base product for NREMS. The Naval Network Warfare Command approved the use of the AMHS.

In May 2004, the Naval Network Warfare Command halted the planned shift of DMS customer support, server operations/maintenance, and client upgrades under the NMCI CLIN 21 process.³ This paved the way for the NMWG to determine an appropriate solution for the Navy's messaging requirements.

2. Naval Messaging Working Group

In July 2004, the NMWG, led by the Space and Naval Warfare Systems Command (U.S. Navy), presented a decision brief to the Naval Network Warfare Command on the implementation plan for NREMS. As will become evident in later chapters, NREMS is only an architecturally different implementation of DOD's mandated DMS. NREMS is still DMS, simply web-enabled instead of a client-server architecture. Therefore, the Navy's messaging business process is still consistent with the architecture outlined by DOD's Global Command and Control System. It is not a stove-piped system unable to operate with the messaging systems of the other military services.

The implementation plan recommended by the Space and Naval Warfare Systems Command (U.S. Navy) included the following key attributes:

³ Cited from the Commander Naval Network Warfare Command Message dated May 10, 2004.

- Consolidation of the Navy's 23 DMS service provider sites to six regional message centers (Naval Computer and Telecommunications Area Master Station, Atlantic; Naval Computer and Telecommunications Area Master Station, Pacific; Naval Computer and Telecommunications Area Master Station, Central Europe; Naval Computer and Telecommunications Station, Far East; Naval Computer and Telecommunications Station, San Diego; and Naval Computer and Telecommunications Station, Bahrain). In December 2004, The Naval Network Warfare Command recommended consolidation of the six sites to two sites (Naval Computer and Telecommunications Area Master Station, Atlantic and Naval Computer and Telecommunications Area Master Station, Pacific) with the possibility of retaining the Naval Computer and Telecommunications Station, San Diego if the two sites cannot support the needs of NREMS.
- DMS client/server and legacy message users will transition to a web-enabled system that eliminates the DMS client software and FORTEZZA at the command desktop. Instead, NREMS will use an Automated Message Handling System (AMHS), a Defense Information Systems Agency (U.S. DoD) approved DMS core product.
- Optional email distribution to support the transition of command business processes including automatic message generators and parsers (e.g., the Global Command and Control System-Maritime).
- Automation of high precedence message notification.

Under this plan, the test sites for NREMS were Naval Computer and Telecommunications Station, Far East and Naval Computer and Telecommunications Area Master Station, Pacific. The pilot system was installed at Naval Computer and Telecommunications Station, Far East in February 2005. The focus of the transition is shore-based DMS implementation that is web-enabled. Afloat forces will be addressed at a later date.

The Naval Network Warfare Command published the NREMS Implementation Plan via a Commander, Naval Network Warfare Command Message dated July 9, 2004. The message outlined the plan and actions required of responsible parties: the Naval Messaging Working Group provides operational direction, the Office of the Chief of Naval Operations secures long term funding and Space and Naval Warfare Systems Command (U.S. Navy) develops, updates and executes the implementation plan.

B. NREMS PROJECT

The Commander, Fleet Forces Command created the requirement for an improved Naval messaging process. The Naval Network Warfare Command, the Naval Messaging Working Group, and the Space and Warfare Systems Command defined the goal and features of the future Naval messaging process. The following discussion will explain the goal and features of the NREMS project.

1. Goal

The goal of the NREMS project is a common messaging service that offers centralized management, improved configuration management, a simplified user interface and results in some cost savings.

2. Features

The NREMS project fulfills the stated goal by reducing the number of sites and supporting personnel (cost savings), providing a system that can support the Net-Centric Enterprise Services strategy with a joint DMS core product (improved configuration management) and providing common business practices. NREMS also provides a simplified user interface with a single message store at a regional node.

a. *Site and Manpower Reduction*

NREMS requires a minimum number of messaging centers reducing the number of sites from 24 to 2. The personnel and resources required to support messaging at the additional sites can now be eliminated with appropriate resources, expertise, and manpower allocated and centralized at the two remaining sites.

Additionally, client software and FORTEZZA cards will not be required at the command desktops. Command resources and manpower can be reallocated to support other requirements.

b. *Consistent with Net-Centric Enterprise Services (NCES) Strategy*

NCES enables information sharing by connecting people and systems that have information to people and systems that need information. For people who have information, NCES provides global information advertising and delivery services. For people who need information, NCES provides global services to find and receive information. NCES requires that data be visible, accessible and understandable primarily through the use of XML tagging. Additionally, information must come from a trusted source and be provided in a format that is interoperable with other systems. NCES must also be responsive to user needs and requirements.

NREMS will migrate Naval messaging to two Naval message stores that can be easily tagged and referenced using appropriate key words. Not only will messages be available for retrospective search within NREMS, but easily accessed by an information consumer through a metadata registry. An information consumer can access information

of interest about any topic, for example, all weather or intelligence messages about a particular region of Iraq. NREMS messages would be sent using NREMS, but would also be available to NCES users through a federated search.

Conceptually, DISA envisions that most Navy organizational messaging will be indexed and stored in a data repository that will create a metadata card for each message for use by the federated search catalog as a reference.

c. Joint DMS Core Product

With the selection of the Defense Information Systems Agency's (U.S. DoD) AMHS DMS core product, NREMS remains an interoperable messaging system and fulfills the architecture requirements of the Global Command and Control System. It remains a joint DOD product.

d. Single Message Store at a Regional Node

The Naval Computer and Telecommunications Area Master Station, Pacific will warehouse all messages for the Pacific Theater and house the backup servers for the Atlantic Theater. The Naval Computer and Telecommunications Area Master Station, Atlantic will warehouse all messages for the Atlantic Theater and house the backup servers for the Pacific Theater. The entire message store for Naval messaging will exist at both sites in the event that one site's service is interrupted. The Naval Computer and Telecommunications Area Master Station, Pacific and The Naval Computer and Telecommunications Area Master Station, Atlantic are redundant message stores.

e. Common Business Practices

NREMS eliminates client software and FORTEZZA cards at the command desktop. Commands are no longer required to update local client software or maintain control of FORTEZZA cards. The software and FORTEZZA cards will be resident at the Naval Computer and Telecommunications Area Master Station, Pacific and the Naval Computer and Telecommunications Area Master Station, Atlantic. Messages will be accessed through a web portal which eliminates inconsistent software and hardware configurations across Naval messaging. Messages can be sent and received from any personal computer with a web browser by authorized personnel appropriately registered with the NREMS website.

C. CURRENT STATUS OF NREMS

The original implementation plan called for implementation in the Pacific theater in fiscal year 2006 (FY06). An NREMS FY 06 budget cut reduced implementation efforts to lab testing and certification. The lab testing began in August 2006 at the Space and Naval Warfare Systems Command (U.S. Navy), San Diego and is on-going. The actual installation was moved to FY 07.

Procurement of all software and hardware is complete as well as award of NMCI CLINs in support of NREMS. Each of the two sites will receive 90 servers, 8 racks and 58 additional hardware components to support NREMS implementation. NMCI will provide the connectivity between the NREMS servers and the NMCI switch, installation of a

DMZ between the NREMS servers and the internet, and authority to install Active X controls on all NREMS work stations.⁴

Implementation is scheduled to begin in the Pacific theater with the installation of all hardware and software required at the Naval Computer and Telecommunications Area Master Station, Pacific. Additionally, the backup servers will be installed at the Naval Computer and Telecommunications Area Master Station, Atlantic for the Pacific theater before the transition can begin. Small commands will be brought online first. Starting with the smaller commands gives the Space and Naval Warfare Systems Command (U.S. Navy) the flexibility to adjust as necessary as they observe the impact on NREMS bandwidth and any unforeseen events. Implementation will progress one command at a time and is not intended to move forward until each command is brought completely online. NREMS is scheduled to be fully operational in November 2008 (see Figure 1).

⁴ Bob Delizo, *Navy Regional Enterprise Messaging System (NREMS) Program Status Presentation*. (12 February 2007).

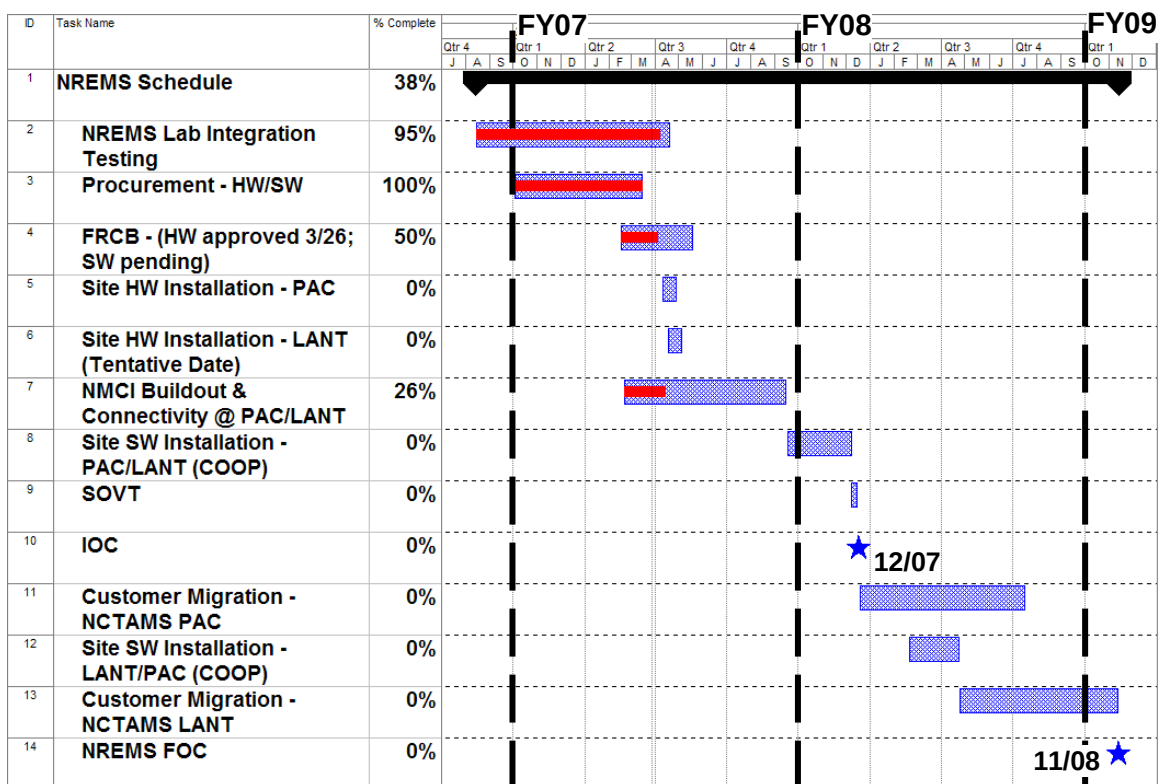


Figure 1. NREMS Implementation Schedule⁵

The command transition plan as outlined by the Space and Naval Warfare Systems Command (U.S. Navy) is as follows:⁶

1. A command submits an NREMS Organization Registration Form to the DMS Service Provider (DSP).
2. Command users and command message administrators (CMA) complete online training courses.
3. The DSP generates an X.509 form and new certificate for the command (PKI certificate).
4. DSP installs the command's certificate on NREMS.
5. The CMA configures user accounts, permissions and profiles.

⁵ Bob Delizo, *Navy Regional Enterprise Messaging System (NREMS) Program Status Presentation*. (12 February 2007).

⁶ Ibid.

6. Command users login to accounts and confirm access.
7. The DSP transitions the command in the DMS directory from a DMS user to an NREMS-DMS user.

When all of the above steps are successfully completed, a command has transitioned from DMS to NREMS.

D. FUTURE STATE OF NREMS

Once shore-based commands have successfully transitioned to NREMS, it is hoped that the transition can be extended to afloat commands as well. The Commander, Fleet Forces Command endorsed a fleet requirement for two-way IP based messaging. DMS and NREMS cannot fully support this requirement yet. Once resolved, NREMS can move forward afloat.

The AMHS in concert with NCES will be updated with the federated search capability. AMHS databases will be provided with a "side door" merge as well to support the NCES strategy of a network-based information environment that will meet the requirement for information superiority and decision superiority. The side door will allow easy access to all AMHS databases by the federated search engine.

III. CHANGE MANAGEMENT FOR DOD COMMUNICATION SYSTEMS

As one can imagine, there are numerous texts on change management and many approaches. This thesis will focus on one approach advocated by Jick of the Harvard Business School. Through this research, he has developed his Ten Commandments of Implementing Change.⁷

1. Analyze the organization and its need for change.
2. Create a shared vision and common direction.
3. Separate from the past.
4. Create a sense of urgency.
5. Support a strong leader role.
6. Line up political sponsorship.
7. Craft an implementation plan.
8. Develop enabling structures.
9. Communicate, involve people, and be honest.
10. Reinforce and institutionalize change.

In this chapter, we will discuss the Navy's transition from DMS to NREMS and compare the Navy's approach with Jick's Ten Commandments.

A. CATALYST FOR CHANGE

In April 2003, the DOD's Inspector General identified several weaknesses in DMS Release 2.2. DMS Release 2.2 could not meet all twelve Multicommand Required Operational Capability (MROC) 3-88 messaging system requirements. (See Table 1). DMS could not process and protect all messages at the appropriate level of security. Classified messages could be transmitted on the unclassified side without detection. Messages might or might not be delivered to the intended recipients if delivered at all. During panel

⁷ Todd D. Jick, *Managing Change: Cases and Concepts*. Homewood, IL: Irwin, 1993, Module 3, for a more thorough explanation of his ten commandments.

discussions, the Navy noted message non-delivery as a significant issue. Message integrity could not be guaranteed. No safeguards existed to protect messages from interception or alteration. Adequate measures were not in place to assure the availability and reliability of DMS. The IG report did note that each of these issues would be resolved by DMS Release 3.0. However, in discussions with SPAWAR, non-delivery notifications and protection of messages at the appropriate classification level are still issues of concern, although improved.

1. Connectivity/Interoperability: Allow user to communicate with any other user within the DMS community and provide system users with standard interfaces to other Government agencies, allies, Defense contractors, and other approved activities external to the DMS community.
2. Message Delivery: System must deliver messages to the intended recipient(s) with a high degree of certainty. System must notify the sender when unable to deliver a message and provide message accountability and traceability from writer to reader.
3. Timely Delivery: System must provide at least two levels of precedence and transmission priorities and at least two levels of importance indicators. System must provide support for changing traffic loads and conditions in time of peace, crisis, and war, such that all messaging characteristics continue to be achieved.
4. Confidentiality/Security: System is to provide the capability to process and protect all message traffic, to include unclassified, classified, and sensitive messages at appropriate security levels and compartments.
5. Sender Authentication: System must have the capability to unambiguously verify and prove that information marked as originating at a given source did, in fact, originate there.
6. Integrity: Information received must be the same as the information sent and the system must provide the user with a selectable verification mechanism.
7. Availability/Reliability: System must provide users with a message service on a continuous basis.
8. Training: System must be flexible and responsive enough to allow the user to operate DMS without extensive training.
9. Identification of Recipients: System must allow sender to unambiguously identify the intended recipient by organization or individual.
10. Message Preparation Support: Preparation of messages for transmission must be user-friendly and allow the use of external message editors.
11. Storage and Retrieval Support: System must have the capability to support storing messages after delivery to allow retrieval for such purposes as forwarding and resending and to support automated message handling functions.
12. Distributions, Determination, and Delivery: System must provide the message originator with the capability to specify special handling and delivery instructions. It also must support single and multiple deliveries, as well as single address lists that result in multiple deliveries.

Table 1. DMS Multicommand Required Operational Capability (MROC) 3-88 Requirements

The IG report also noted that the cost savings of \$435 million originally estimated for the transition from AUTODIN to DMS were not realized. The aging and antiquated AUTODIN system continues in use along with DMS. Two systems are being supported simultaneously until AUTODIN is

completely phased out and DMS fully implemented. AUTODIN was originally scheduled to be phased out in 2000, however, its use continues because DMS cannot fully meet the system requirements of MROC 3-88. Unfortunately, the funding for legacy systems (AUTODIN) will not continue beyond fiscal year 2011 (FY11).⁸ It is now imperative that DMS meet the system requirements outlined in MROC 3-88 and produce cost savings well before FY11.

Recognizing the operational and fiscal challenges faced by naval messaging, the Commander, Fleet Forces Command initiated its change requirement in the Commander, Fleet Forces Command Message dated October 14, 2003 as discussed in Chapter II. Note that many of the DMS system issues identified by the DOD IG report are also identified as system criteria by the Commander, Fleet Forces Command, primarily performance and security.

B. ROLES OF CHANGE PARTICIPANTS

Every member of an organization involved in business process reengineering or organizational change has a role. Change can only succeed if all members are active, involved and committed during the process of change. Even the naysayers play a valuable part in the process. They can illustrate the weaknesses of any change plan and recommend some of the best solutions for solving or mitigating them. For the purposes of our discussion, change participants fall into three broad action roles: change strategists, change implementors, and change recipients.⁹

⁸ As discussed with the Space and Naval Warfare Systems Command (U.S. Navy) during a phone conference in August 2006.

⁹ Jick, Module 3, for more explanatory information on change agents and their roles.

The change strategists are those responsible for initiating the change. They identify the need early on, create the vision and desired outcome, describe the extent of the change, select change sponsors, and defend the change requirement. The Commander, Fleet Forces Command identified the need for a shift from the current naval messaging process, DMS, to a new naval messaging system. Their message clearly articulates their vision and desired outcome. They described the extent of the change by identifying performance evaluation criteria of any proposed system. The Naval Network Warfare Command was selected as the change sponsor who later created the NMWG which is responsible for the operational direction of the NREMS project. Later, the NMWG restricted the extent of the change to an AMHS DMS core product implemented ashore only. Programmatically, the change is easy to defend for all of the reasons outlined in the DOD IG report as well as evidenced by the actual performance of DMS. Culturally, however, the change is more difficult as will be discussed later in this chapter.

Change implementors provide the bulk of the work in any change process. Their efforts can make or break any change effort. Change implementors manage the day to day process of change. For the NREMS project, the Space and Naval Warfare Systems Command (U.S. Navy) is responsible for developing, updating and executing the implementation plan. The Space and Naval Warfare Systems Command (U.S. Navy) provides the day to day effort required to shape, enable, orchestrate and facilitate change progress. Without their efforts, the change could not progress.

Change recipients represent the largest group of people in any change endeavor. Change recipients must adopt and adapt to the change. If change recipients do not institutionalize the change, the change cannot successfully occur. Instead, change recipients will revert to old habits either delaying the inevitable change or prohibiting the change from occurring at all. Naval commands and registered naval messaging users who must adopt and adapt to NREMS are the change recipients of the NREMS project change endeavor. Already at odds with DMS, this group of individuals will be the hardest group to commit to the transition from DMS to NREMS.

During the NREMS project transition discussion, it is important to remember each of these roles and the responsibilities each has toward the success of the change.

C. AN ANALYSIS OF THE NREMS PROJECT CHANGE MANAGEMENT APPROACH

Jick's Ten Commandments will form the framework of analysis for the change management approach of the NREMS project. Therefore, a brief explanation of Jick's Ten Commandments is appropriate. Once explained, the salient points of the NREMS project transition plan will be discussed with respect to Jick's framework. The discussion will focus both on the strengths and weaknesses of the approach. Chapter VII will provide the conclusions of the analysis.

1. The Ten Commandments of Implementing Change

The following section is provided to develop a common understanding of Jick's Ten Commandments prior to analysis of the NREMS project.

a. *Analyze the Organization and its Need for Change*

An organization, its structure and habits, must be fully understood before any change can occur. Change strategists must understand a process's current state, strengths and weaknesses before determining whether change is, in fact, necessary.

b. *Create a Shared Vision and Common Direction*

A central vision of any proposed change helps to unite the organization and focus their efforts toward change implementation. The shared vision provides change participants with a destination or goal.

c. *Separate from the Past*

It is imperative that any organization disengage from past behavior, habits and routines that do not move the organization forward or inhibit it. However, many find comfort in the known and predictable. Develop reward systems that support desired behaviors and end states. Do not reward old habits or routines that do not support the change endeavor.

d. *Create a Sense of Urgency*

One organizational change expert outlines two prerequisites for successful organizational change which are quoted below:¹⁰

1. Pain: a critical mass of information that justifies breaking from the status quo.
2. Remedy: desirable, accessible actions that would solve the problem or take advantage of the opportunity afforded the current situation.

¹⁰ Daryl R. Conner, *Managing at the Speed of Change*. New York: Villard Books, 1992, Chapter 6, for an explanation of the process of change.

It is this pain and the proposed remedy that create the sense of urgency required to initiate change momentum.

e. Support a Strong Leader Role

Change requires an inspirational leader to guide and drive change efforts, someone or some entity that effectively and enthusiastically advocates for and defends the change effort. Without a strong leader, many change endeavors flounder and fail.

f. Line Up Political Sponsorship

Often, we misunderstand the term "political sponsorship." Political sponsorship not only refers to senior leadership, but all organizational members. Who are the informal leaders of the process under transition? Have they been included in the change process? Did they participate in selecting the appropriate solution and developing the implementation plan?

g. Craft an Implementation Plan

The implementation plan is the framework and timeline required to implement change. It identifies roles, responsibilities, and activities/timelines required to implement the change. It should be specific and detailed enough to be clear, but flexible enough to change as circumstances dictate. It should be a living document that is continually revised as new information is made available, and successes and setbacks occur during the change process.

h. Develop Enabling Structures

Enabling structures are designed to spotlight and facilitate change. These structures can include pilot tests, off-sight workshops, training programs and feedback mechanisms that support change. The more complex the

change, the more thought out the enabling structures need to be to ensure that they support each other and are consistent with the vision of the change.

i. Communicate, Involve People, and Be Honest

All change participants should be made aware of the proposed change as soon as practically possible. Care should be taken in how the change is introduced. Do not gloss over the difficulties that can and will be faced. As discussed in commandment four, focus on the necessity of the change and the benefits of the solution for the change recipient.

j. Reinforce and Institutionalize Change

Change is required for any organization to remain competitive in their field of endeavor. Although we want to institutionalize the changed process, we truly need to institutionalize a culture receptive to change. These cultures more readily institutionalize new systems and processes and view change as a positive and important endeavor that sustains the organization and helps it proliferate.

2. Analysis

It is not necessary to address all Ten Commandments when analyzing any change endeavor. The Ten Commandments are meant simply to be a guideline, not a roadmap for success. With this in mind, this section will address some of the more salient characteristics of the reference framework as they apply to the NREMS project.

Although we fully understand the limitations, strengths and weaknesses of DMS, we do not fully understand the actual architectural structure of DMS in the Navy. No clear inventory or system diagrams exist to paint a picture

of how DMS software and hardware have been implemented at the organizational level. One individual at the Naval Computer and Telecommunications Area Master Station, Atlantic indicated that any past survey efforts have met with lackluster results. Either naval messaging organizations don't know what they have or do not have the resources to clearly articulate their assets. The current NREMS implementation plan is based on an educated guess of the assets that exist. As with past change efforts from AUTODIN to DMS, or NMCI, the lack of knowledge about actual assets can be very problematic resulting in time delays and additional resources. It can also result in significant change recipient push back as roadblocks are encountered when the lack of understanding of the current system and structure become evident.

SPAWAR understands this weakness and has plans in place to help mitigate any potential problems down the road. The change will occur in the Pacific Theater first before it moves into the Atlantic theater. Smaller commands are targeted to transition first so that bandwidth can be monitored and potential problems with existing systems and infrastructure can be managed in a more controlled environment. As problems are encountered, time will be taken to identify appropriate solutions before moving forward. A command can be easily shifted back to DMS until issues are resolved minimizing impact to the messaging capabilities of that command. No more than one command should be affected at any one time. Because the NREMS project is simply a shift from a client-server based DMS to a web-enabled DMS system, the issues encountered should be minimal.

Commander, Fleet Forces Command set forth a clear vision in their October 2003 message and the Naval Network Warfare Command, the NMWG and the Space and Naval Warfare Systems Command (U.S. Navy) have developed an implementation plan that achieves this vision. However, few change recipients are aware of the message or the vision. Even fewer understand the difference between DMS and NREMS.

At one command we visited, a registered naval messaging user had no idea what NREMS was or that a transition would be occurring within naval messaging. Significant resources are available on the naval messaging website that outline NREMS and provide training for AMHS. However, he was completely unaware of NREMS, its vision or its benefits to his command like reduced maintenance requirements. When introduced to the NREMS project, he immediately became skeptical of any need for change. With little knowledge of NREMS, he was already resistant to the idea of NREMS.

Although AUTODIN is antiquated and aging, it works and still performs functions that DMS cannot. Organizations were, and still are, resistant to letting it go. "If it's not broke, don't fix it." Few are aware of the costs and limitations associated with maintaining this system. Even fewer are aware of the benefits of implementing NREMS vs. AUTODIN or DMS.

In order for change to be effective, we must reinforce those behaviors and actions that we desire, i.e., transitioning to NREMS. Instead, we reward individuals who will maintain a naval messaging capability whether with AUTODIN, DMS, NREMS or any method that allows messages to

be successfully sent and received. As anecdotal evidence I present an example presented to me by the Projects Officer (N5) at NCTS Puerto Rico during the transition from AUTODIN to DMS:

NCTS Puerto Rico was ordered to transition from AUTODIN to DMS. However, the Naval Computer and Telecommunications Station, Puerto Rico did not have the infrastructure to support the transition. Because this mandate was urgent, she developed workarounds in order to implement DMS. The goal of DMS, however, was standardization of DOD messaging hardware and software. The standard hardware and software architecture could not be implemented because the infrastructure at NCTS Puerto Rico could not support the bandwidth requirements of DMS. Additional hardware, not specified by the DMS program, was purchased to allow NCTS Puerto Rico to communicate with other DMS activities. In spite of the non-standard implementation of DMS, the Projects Officer received an award for implementing DMS on schedule and within budget.

Members of Navy organization are routinely rewarded for behaviors that are not consistent with the vision of most change efforts. Successfully completing a mission is considered more important than the method used to complete it. It is difficult to successfully move forward while rewarding past bad behavior. Do we have an appropriate reward system in place to support the transition from DMS to NREMS? What behaviors should be rewarded?

Most change participants (change strategists and change implementors) from the Commander, Fleet Forces Command to the NMWG and the Space and Naval Warfare Systems Command (U.S. Navy) feel the pain induced by the inadequacies of DMS to meet the Navy's needs and the fiscal burden of maintaining legacy systems in conjunction with

DMS. They also understand the rewards of the remedy: decreased maintenance costs and requirements, decreased manpower requirements, consistent configuration implementation, and a reduced number of assets required to operate NREMS.

Navy organizational messaging commands (change recipients) only understand the pain they endured during the transition from AUTODIN to DMS with the proposed transition from DMS to NREMS coming down the road. In numerous discussions, we heard the question, "Why are we transitioning again when we couldn't get DMS to work?" Change recipients do not perceive the same pain as change strategists and change implementors, nor are they aware of the rewards of the remedy. The available literature outlines the structure of NREMS, not the requirement for it or the benefits of the transition.

The NREMS project included both a test lab at the Space and Naval Warfare Systems Command (U.S. Navy), San Diego and a pilot site at the Naval Computer and Telecommunications Station, Far East. AMHS was tested in a lab environment before fielding at the test site. Care was taken to ensure that NREMS had the same look and feel as DMS. The browsers are virtually identical with minor differences that are easily navigated. Issues discovered during the test pilot were brought back to the testing lab for verification and resolution.

The NMWG has planned a significant training program for NREMS users. Personnel at both messaging centers will receive in-class training. NREMS CMAs and users can register for on-line courses that will be made available.

As commands transition, experts will be present to provide initial orientation and ad hoc training as required.

With the exception of the pilot project at the Naval Computer and Telecommunications Station, Far East, no significant feedback system is in place. While visiting the testing lab in San Diego in March 2007, the question was posed, "How do I comment on AMHS, ask questions or provide input once I've visited the website?" At that time, no formal feedback system existed. A help menu was available, but could not address unique or specific questions. It provided general knowledge only. This can easily be remedied by simply providing a link to an email address for feedback submission. However, it is extremely important to provide change recipients with an effective feedback mechanism. This simple change requirement cannot be overlooked.

Change recipients' are still reeling from the effects of the transition from AUTODIN to DMS. It will take significant communication to convince them of the need to transition from DMS to NREMS. Communicate the change in a manner that speaks to the change recipient, i.e., maintenance and upkeep will shift from the command to the message center with a web-enabled messaging system, fewer resources will be required by commands to maintain the messaging capability, etc. Address issues that are of concern to the change recipient. Keep in mind that change recipients' issues may not be the same as the issues concerning change strategists and change implementors.

No change solution will please everyone. However, if change recipients understand the strengths, weaknesses and resource limitations (i.e., funding constraints, available

technology, federal guidelines/mandates, etc.) of the solution, they are more likely to commit to the change and institutionalize it.

As mentioned previously, extensive literature is available on the naval messaging website about NREMS. The literature does not include information that would help to create a sense of urgency among change recipients. It is also unclear how extensively it is accessed.

Initially, the Space and Naval Warfare Systems Command (U.S. Navy) had planned a "road show" to introduce the NREMS transition, answer questions, and provide an informal feedback mechanism. Unfortunately, limited resources have forced the Space and Naval Warfare Systems Command (U.S. Navy) to cancel this effort. Studies have shown that implementation shortcomings include:¹¹

- Failing to win adequate support for change.
- Neglecting to involve all those who will be affected by change.
- Dismissing complaints outright, instead of taking the time to judge their possible validity.

The funds expended initially to conduct the road show may actually mitigate the long term cost of not gaining initial change recipient support. Change recipient push back can cause extensive implementation delays and expenditure of a large amount of resources. A thorough risk analysis should be conducted to analyze the potential impact of change recipient push back. Are the costs associated less than the cost of a road show?

The shift from DMS to NREMS will not require significant business process reengineering. Change

¹¹ Jick, Module 3, for more details of the study.

recipients will perform the same functions within NREMS as with DMS, only with less effort because of the transition to a web-enabled system, less hardware and software requires less maintenance and resources. If made aware of the benefits of the transition, it is expected that the benefits should be sufficient to institutionalize the change. Without this knowledge, change recipients will not be receptive initially and can delay implementation efforts. Skepticism is only overcome by sufficient information and contextual knowledge.

D. CONCLUSION

The NREMS Project fulfills many of the requirements for a successful change endeavor: a vision with a common direction, a sense of urgency (among change strategists and change implementors), a thorough implementation plan, a strong leader role (the NMWG guides implementors) and enabling structures. However, there is a significant gap between change strategists/implementors and change recipients.

Kirkpatrick defines three keys to a successful change: empathy, communication and participation.¹² Surprisingly, each of these keys are with respect to change recipients. Strategists initiate and guide the change, implementors execute the change, but recipients institutionalize the change. It is imperative that change recipients are adequately informed, involved, and provided appropriate feedback mechanisms as early as possible. Too often, change recipients are made aware of the transition as it occurs. This creates unnecessary anxiety and confusion

¹² Donald L. Kirkpatrick, *How to Manage Change Effectively*. San Francisco: Jossey-Bass, 1985, Chapters 6-9, for a more thorough explanation of each key.

even for the most valid change endeavors. Gaining recipient commitment will require more resources and information than is currently available for the NREMS Project.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. REVIEW OF NAVAL MESSAGING ARCHITECTURE

The Naval messaging architecture forms the informational basis for the Navy's requirements for organizational message traffic and the systems of choice to satisfy these needs. In this chapter both the DMS and NREMS messaging architecture will be reviewed with regard to four critical factors: strategic concept, operational requirements, problem characterization, and analysis of the architecture. Section 1 will introduce the strategic concept each architecture supports for DOD electronic messaging. The operational requirements, section 2, will be summarized into the proposed operational goals for the success of each system. DMS and NREMS technical, operational, and cost issues will be outlined for further review in section 3. Finally, section 4 will end the chapter with the summarized analysis of the architectural guidance for the systems.

A. DEFENSE MESSAGING SYSTEM (DMS)

The Defense Message System (DMS) is now the DOD's system of record for handling organizational messages¹³ (DISA 2006). Because of their official and often critical nature, organizational messages place specific operational requirements on communications systems such as high level security, precedence, timely delivery, and high availability and reliability. DISA initially planned to implement DMS on over 360,000 desk-top computers at over 7,000 sites worldwide (i.e., tactical forces, allies, Federal Government users, and defense contractors).

¹³ Organizational messages are messages and other communications exchanged between organizational elements in support of command and control (C2), combat support, combat service support, and other functional activities.

Ultimately, the goal of DISA was to extend DMS to over 2,000,000 desktops to provide ordinary email and "individual" messaging using commercial off the shelf standards and technology (DOT&E 1997).

1. Strategic Concept

DMS is structured to provide an interoperable, seamless, and secure electronic messaging system for organizational users within the Department of Defense. DMS uses commercial products for drafting, coordinating, and releasing messages. The system design architecture used to develop DMS provides a flexible framework that is positioned to support evolving requirements (e.g., a modified set of required operational messaging characteristics), a design that is collaborative computing centric, and an implementation that provides both acquisition and life cycle cost reductions. This architecture supports the key DMS design tenet: a single messaging solution for DOD electronic messaging (LMC 2004).

The Target Architecture and Implementation Strategy TAIS) describes DMS as an evolutionary (incremental development strategy employed) that engages a joint DOD process to coordinate requirements, architecture, policies, standards, funding and acquisitions. Using a phased development plan for the transition, the strategic aim is for the DMS architecture to achieve near-term cost and personnel savings while enhancing DOD's messaging capability through a jointly-developed (cross-Service and Agency involvement) system (DMSAWG 1990).

2. Operational Requirements

The Multicommand Required Operational Capability (MROC) 3-88 Change 2 outlines several operational goals for DMS to achieve as a system. DMS should:

- a. Provide message service to all DOD, and interface with other U.S. Government agencies, allied countries, defense contractors and other authorized users (e.g., academia).
- b. Process and protect all unclassified, classified, and sensitive message traffic at all levels and compartments based upon integrity, authentication, and confidentiality.
- c. Provide standardization and interoperability, while preserving adaptability to implement Service and agency unique functions.
- d. Be backward compatible with the AUTODIN system (including base-level support systems) and the electronic mail systems on the DOD Internet.
- e. Support a guaranteed secure and timely delivery of organizational message traffic, based upon precedence, to its intended recipient; with prompt notification of non-delivery.
- f. Adapt to changes in users capacity, component upgrades, connectivity and message throughput without major redesign or steep user learning curves, while preserving the ability to implement Service and agency unique functions.

These capabilities are expected to promote a messaging system superior to Automatic Digital Network (AUTODIN) toward contributing to information superiority.

Specifically, the MROC 3-88 defines 12 general operational requirements for DMS to address in its messaging function:

1. Connectivity/Interoperability
2. Message Delivery
3. Timely Delivery
4. Confidentiality/Security

5. Sender Authentication
6. Integrity
7. Availability/Reliability
8. Training
9. Identification of Recipients
10. Message Preparation Support
11. Storage Retrieval
12. Distribution Determination and Delivery.

In this research, the operational goals and the messaging characteristics established by the MROC 3-88 Change 2 will be reconciled to help assess the critical quality attributes that significantly contribute to the success or failure of the system.

3. Problem Characterization

The expected outcome from implementing the DMS system is to reduce cost and staffing by eliminating the outdated and expensive AUTODIN system. This earlier system was implemented in 1962 to provide DOD secure and reliable transmission of organizational messages. In a late 1980s study, the Defense Information Systems Agency (DISA) concluded that AUTODIN was inflexible, outdated and costing in excess of \$700 million per year to operate (NCS 2000). To reduce costs, DMS was expected to fulfill the tactical and allied messaging role by using available commercial products and incorporate industry standards.

According to the results of independent operational tests conducted by the Joint Interoperability Test Center (JITC), DMS Release 2.2 (April 2001) did not fully meet four of the 12 MROC requirements: confidentiality/security, message delivery, integrity, and availability/reliability. The release of DMS 3.0 (June 2002) was developed to satisfy these MROC requirements and with continued product

improvements these shortfalls are becoming less relevant to DMS success, according to the JITC (2002) testing completed.

The most costly problems of the system appear to be maintenance and support. The DMS architecture uses a client-server model based on Microsoft Exchange and the Outlook client, the client-server model has posed problems for the system. A white paper proposing an alternative solution, "Background of the Naval Regional Message System (NREMS)," suggest the following DMS limitations:

a. DMS Client Maintenance

In addition to customer problems, the client maintenance complexity has created a greater support burden for the DMS program than desired. The DMS client requires regular and sometimes complex patches / configuration updates.

b. FORTEZZA Logistics

Considerable logistical coordination is also required to distribute and maintain the FORTEZZA cards¹⁴ required for operation with the DMS client software.

4. Analysis of Architectural Guidance

From the earliest development phase, DMS has used an architectural design approach. This specific approach addresses the operational requirements previously presented, but also considered important aspects needed in the overarching DMS architecture. The following is a

¹⁴ Fortezza cards are 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 (CMS-9).

summary of the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5721.01C established minimum architectural criteria, DMS should:

- a. Promote interoperability with previous versions of DMS and other messaging systems.
- b. Be extensible by supporting multi-location groupware designs that take advantage of capabilities in commercially available collaborative computing products.
- c. Be scalable toward future improvements that prevent product limitations from negatively impacting system reliability, scalability, security, and performance.
- d. Reduce the cost to operate, manage, and support the fielded system.

B. NAVY REGIONAL ENTERPRISE MESSAGING SYSTEM (NREMS)

The Navy Regional Enterprise Messaging System (NREMS) is an enhancement to the Defense Message System (DMS) architecture. NREMS will provide the capability for ashore users to send and receive DMS messages using a web browser. NREMS will eliminate the need for possessing DMS FORTEZZA cards by the end users and eliminate the very often and sometimes complex software patches and configuration updates at the end user site. With the implementation of NREMS, the Navy seeks access to reliable, decision-quality organizational messaging through network-based messaging services.

1. Strategic Concept

The strategic concept is a centralized Navy DMS messaging architecture operating through regional messaging centers, which profile messages for customer commands, manage FORTEZZA cards, work non delivery notice (NDN) issues, and provide training and assistance as required. An enterprise solution will mitigate existing DMS operations and maintenance issues by eliminating client software, and

consolidating FORTEZZA cards, Navy DMS messaging and its expertise at the regional sites. The end state will move complex messaging tasks from non-information technology personnel to trained messaging professionals, and will allow a reduction in the number of local control centers (LCC's) and regional server sites (RSS's). This presents an opportunity to mitigate issues with DMS installation, operations and maintenance, and to improve governance, performance, security and cost. Implementation of NREMS will allow the Navy to consolidate to a two (2) site Regional Navy Operational Service Center (RNOSC) from the current eight (8) DMS Service Provider (DSP) sites. NAVNETWARCOM (NNWC) plans to implement NREMS at NCTAMS PAC (Wahiawa, HI) and NCTAMS LANT (Norfolk, VA) with full failover between these sites (COMNAVNETWARCOM 152158Z DEC 04). NREMS provides an enabler for Network Centric Enterprise Services (NCES) in support of the Global Information Grid Enterprise Services (GIG-ES) (PEO C4I 2005).

2. Operational Requirements

In response to DMS problems characterized within section A.3 of this chapter, Commander, Fleet Forces Command released a message requesting the Navy to evaluate the Automated Message Handling System (AMHS) as a standard Navy enterprise DMS messaging solution (Commander, Fleet Forces Command 221414Z OCT 03). The primary basis for the NREMS requirements continue to stem from the MROC 3-88 Change 2 but defines organizational messaging requirements based upon a standard enterprise messaging solution for medium to large commands. The messaging community recommended consolidating the existing messaging infrastructure and web-enabling DMS messaging. The AMHS, a

product suite developed by the Telos Corporation, was selected for implementation. The Telos AMHS is part of the jointly tested and supported DMS core baseline set of products. The technology is mature and has been developed and tested by DISA and used with organizations such as Combatant Commanders (COCOMs) i.e., PACOM. NREMS presents an opportunity to re-architect DMS in order to resolve installation, operations and maintenance issues. The AMHS Operational Concept Document suggests that with the use of the CP-XP/Telos AMHS (and Domain FORTEZZA) the following functional advances can be realized:

- a. Relieve the end user of the requirement to maintain the DMS User Agent (UA) client workstation.
- b. Centralize the FORTEZZA function (the user would no longer hold the FORTEZZA card).
- c. Centralize DMS systems management to a reduced quantity of sites (down from the 20+ area communication centers (ACC) and local communication centers (LCC) to six sites or less).
- d. Web enable all processes of message management including reading, sending, archiving, retrospective search, and account management.
- e. Empower the Navy to outsource basic systems management functions to a contractor.

3. Problem Characterization

While NREMS should resolve DMS issues such as site maintenance and FORTEZZA logistical dilemmas, it is not without its program shortfalls. NREMS problems are epitomized by various technology performance and costs constraints that are success factors (PEO C4I 2005). They include the following.

a. NMCI Connectivity

The Navy has directed contractor owned/government operated regional Automatic Message Handling Systems (AMHS) that leverage existing contract vehicles and NMCI infrastructure and aligns with emerging NCES standards (COMNAVNETWARCOM 101644Z May 04). NMCI must be prepared to provide sufficient connectivity, bandwidth and network services to support NREMS.

b. DOD PKI Availability

Implementation of AMHS requires system functions and associated proxy-release policy that permits a web browser-based user to send a message from Microsoft Internet Explore (IE). Some form of security must be implemented to ensure authenticity, integrity and confidentiality for DOD messaging is maintained. DOD PKI can be successfully exploited for use within the Sensitive But Unclassified (SBU) messaging environment, however PKI is not well established in the SECRET messaging domain and completely lacking in the Top Secret/Collateral (TS/C) messaging domain.

c. Multi-user Capability

AMHS software must address user scalability and support the 2 RNOSC concept. The capability to handle thousands of messaging users simultaneously during peace and wartime traffic loads is a mandatory function for the AMHS. Currently the "stress test" to ascertain the maximum user and message generation capacity thresholds has not been conducted.

d. CP-XP Service Restart Time

A re-caching (or revalidation) of stored certifications is performed by this "service" and, based on the number of unique credentials hosted by a particular

AMHS server, can be an operation preventing timely and full return-to-service of the AMHS overall.

4. Analysis of Architectural Guidance

The NREMS planning initiative seeks to transform Naval messaging into a full IP based capability providing access to record message traffic from anywhere at anytime. In order to maintain the same level of service to the fleet, technology investments must be made that will provide the foundation for future transformational communications architectures. NREMS is a web based service to meet OSD mandated Defense Messaging System Requirement. NREMS replaces DMS MS Exchange/Outlook products and many legacy products. NREMS should provide:

- a. Fully joint and allied interoperable messaging capability.
- b. Availability to a secure web based message search capability, with minimal disruption of services, to replace myriad command unique message handling systems.
- c. A system scalable to large-scale enterprise deployment while maintaining full user capabilities; secure reader, drafter, and releaser functionality during peace and wartime operational messaging volumes.
- d. Regional networked product maintainability and manageability for mandatory software and security upgrades.

The discussion of the four critical factors: strategic concept, operational requirements, problem characterization, and analysis of the architecture provides the functional analysis and operational basis for the Naval messaging construct. Despite the architectural differences (client-server vs. network model) the core architectural guidance remains the same. The following chapter will

introduce the research methodologies employed to assist in analyzing the DMS to NREMS architecture implementation. Both architectural analysis and business process re-engineering techniques will be used to examine how well the planned architecture satisfies MROC requirements and the quality goals for the system.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RESEARCH METHODOLOGY

Since the migration of DOD messaging to the DMS has been mandated, implementation has been less than ideal and otherwise unsuccessful. DMS users have reported dissatisfaction with the systems maintenance and security support burdens in the current client-server model (DODIG 2003). NREMS introduces a networked environment capable of push technology and centralized database and security management which should significantly reduce the DMS shortfalls that have made the system lack appeal to the end user. As the DOD seeks to solve these issues, other potential issues are introduced that must be reviewed and addressed to ensure a successful implementation of the NREMS.

Two methods were used in this thesis research. The Architecture Trade-off Analysis Method (ATAM) and user surveys formed the basis for analysis, conclusions, and recommendations. The goal of the ATAM is to understand the current message system, DMS and the consequences of architectural decisions with respect to the quality attribute requirements of the new messaging system (Clements et al., 2000, p. 1). User surveys provided the data to characterize the current naval messaging business process for each naval command and across the Navy with the prospect of properly defining future NREMS users. Combined analysis provided a clear expectation for the alternative architecture to the existing DMS architecture.

A. ARCHITECTURE TRADE-OFF ANALYSIS METHOD (ATAM)

A system is driven by both functional and quality goals. The architecture is the key to achieving—or failing to achieve—these goals. The ATAM not only reveals an architecture's ability to satisfy these particular quality goals but also provides insight into the how the quality goals interact with each, hence the name trade-off analysis method. The ATAM is a nine step process separated into four groups/phases: presentation, investigation and analysis, testing, and reporting (Clements et al., 2002, p. 39). Presentation begins the process with the exchange of information. Investigation and analysis assess the key quality attribute requirements based upon the architectural approach. Testing checks the result of the analysis against the stakeholder needs. Finally, the reporting phase presents the results of the ATAM to the appropriate stakeholders.

This ATAM evaluation will expose architectural risks that potentially inhibit the achievement of an organization's business and mission goals (Bass et al., 2006). This will be accomplished by evaluating the system architecture relative to its system components and quality attribute goals such as security and maintainability. In addition to discovering how well the architecture satisfies quality goals a map of how these quality attributes interact with each will be presented. In the absence of system stakeholders and direct access to a test and evaluation center, only the presentation, the investigation and analysis phase of the ATAM were accomplished for the NREMS architecture (Clements et al., 2002, pp. 44-45).

An abundance of available literature (Bass, Clements) and test results currently exist to address the functional, operational, and architectural requirements of DMS. DMS projects have received a high priority from Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD/C3I) in terms of funding support, since inception, because of its critical importance to defense messaging (DMSAWG, 1990). With top-down support, DMS has evolved to introduce new capabilities and expand to meet MROC 3-88 requirements.

NREMS, unlike DMS, is not a program of record and lacks the personnel and funding support afforded the DMS program. NREMS is solely based upon the requirements set by the DMS MROC 3-88 requirements with featured enhancements to reduce the costs associated with the maintenance and support of the DMS. This analysis will begin with an analysis of the DMS architecture as a frame of reference then attempt to perform an in-depth analysis of the NREMS architecture to determine whether the system is capable of meeting the previously discussed DMS MROC 3-88 requirements within the desired web-based architectural environment.

B. USER SURVEYS

The survey was disseminated to all users registered with the Navy Regional Messaging website (see Figure 1). The sample collected from this population was used to statistically characterize naval messaging requirements, i.e., fully web-enabled messaging with only thin clients on site, messaging requiring the use of a Defense Message

Distribution System (DMDS) locally, or a combination of both. Resources can then be properly allocated and planned to support the transition from DMS to NREMS.

Little is currently known about end user naval messaging business processes. During the transition planning from DMS to NREMS, naval messages were disseminated to naval organizations through NETWARCOM requiring feedback by a due date. Past solicitation of end user requirements and system components have generated lackluster response. The transition from DMS to NREMS was planned utilizing educated guesses of end user requirements of the naval messaging system. True data and system inventories do not exist in any easily accessible database.

In conjunction with the Space and Naval Warfare Systems Command, six end user business processes were defined and characterized in Figure 2. The questions in the survey were crafted to navigate the decision tree and select a specific business process for each respondent (Appendix A). The aggregate of responses was used to characterize the complete business model for naval messaging by determining the percentage of each type of business process present and extrapolating across the entire enterprise. Additional questions were included in the survey that were not relevant to the business process decision tree, but were of interest to SPAWARSYSCOM.

Subject:
Naval Messaging Survey

Message Content:

In an effort to optimize resources and ensure that we can support you appropriately, the Navy Post Graduate school under guidance from PEO-PMW160-3 has developed a survey to help us understand your command's business process for organization messaging. The results of this survey will be used to properly plan, route resources to where they are most needed, and identify an optimum business process for your command as the Navy transitions to a web-based messaging management system called Navy Regional Enterprise Messaging System (NREMS). We appreciate your taking the time to complete this very easy survey.

The link to the survey is:

<http://www.surveymonkey.com/s.asp?u=159313533084>

Further information about NREMS is available in the Naval Messaging Web site located at:

<https://navalmessaging.spawar.navy.mil/>

The survey should be completed by all Commands System Administrators.

The survey should take less than 10 minutes to complete.

The deadline for survey submission is 18 May 07.

The Naval Messaging Web site is located at <https://navalmessaging.spawar.navy.mil/>

Sincerely,

Naval Messaging Web Site Administrator

Figure 2. Naval Messaging Survey email disseminated to all registered NREMS users.

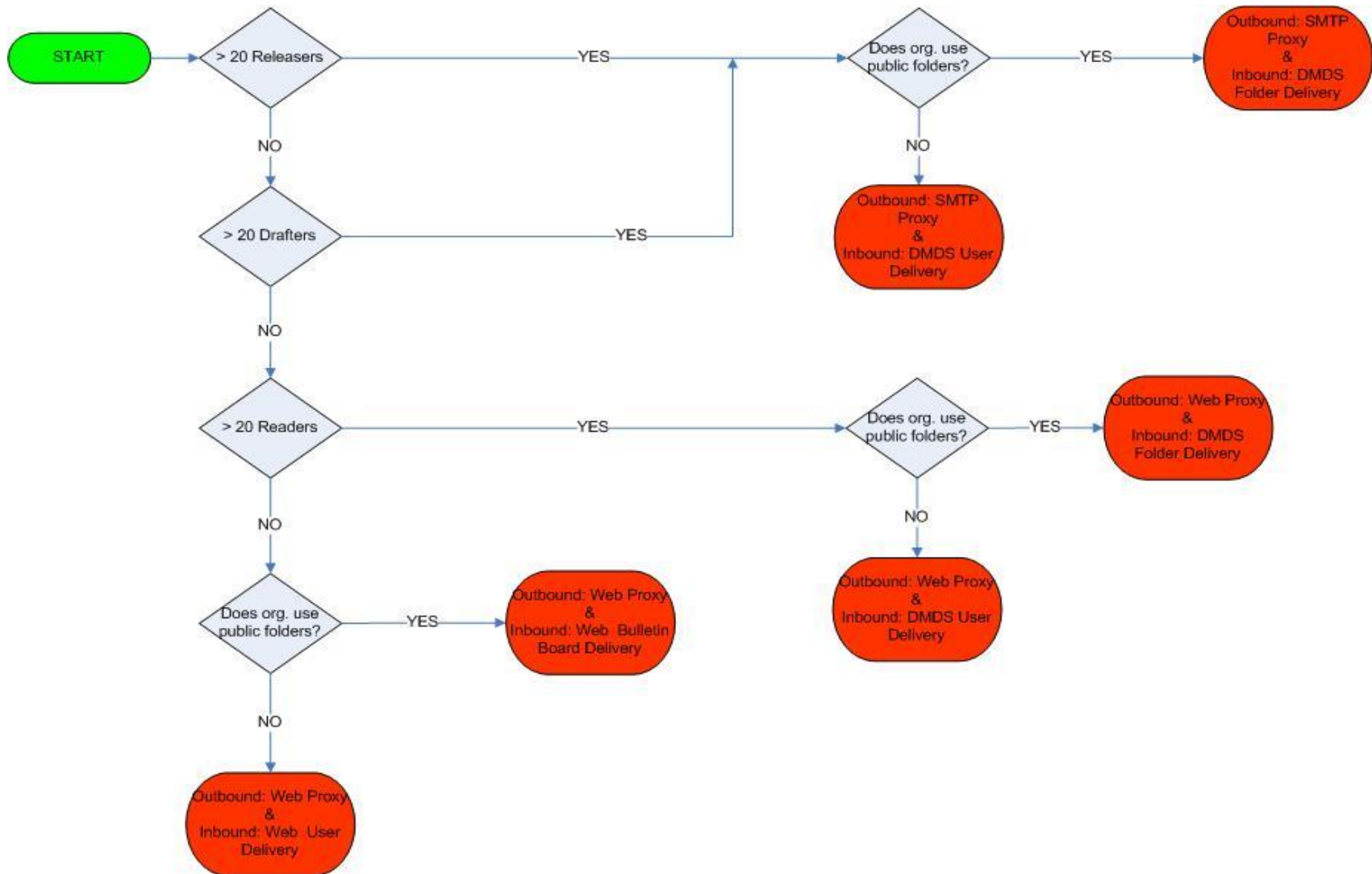


Figure 3. Naval Messaging Business Process Decision Tree (From: SAIC-PEO C4I PMW 160.3)

VI. RESEARCH ANALYSIS

With the emergence of the Internet, and subsequently the Web, messaging now affects business efficiency and competitiveness such that it has become a mission-critical part of enterprise systems. Because messaging is such a fundamental feature for many application architectures, poor choices can have disastrous consequences, affecting performance, scalability, availability, and ultimately user acceptance.

As mentioned in the previous chapter, the DMS architecture will serve purely as a frame of reference for the NREMS implementation within this thesis. The Defense Message System Target Architecture and Implementation Strategy can be used for a more in-depth analysis of the DMS architecture. This thesis will focus the analysis on the additive advantages that NREMS introduces to the DOD as well as introduce architecture and business process shortfalls that could result in a program failure. It will also provide more detailed information about the current structure of naval messaging and the ideal end state for naval messaging organizations after transition to NREMS.

A. DMS ARCHITECTURE ANALYSIS

In preparation for the architectural evaluation, the system is first broken down or presented as individual components and described within the context of each one as an element of the architecture. The current DMS client/server architecture is based on Microsoft Outlook 2000 products and the following components.

1. Message Handling Services (MHS)

The DMS MHS provides the core capability for military messaging. The X.400 Message Handling System (MHS) consists of two subsystems: The core MHS (i.e., those components needed to originate, transmit, receive, and store messages) and specialty products that provide message distribution determination, interoperability with AUTODIN, address list expansion, and interoperability between users on disparate secure networks. It also contains a special directory used to provide centralized message routing management.

2. Directory Services (DS)

DS supports DMS by providing naming, addressing and contact information for messaging. The X.500 Directory System consists of the Directory System Agent (DSA) that hosts its information, applications that access the directory, and an administrative application for directory maintenance.

3. Security Services (SS)

DMS security services integrated throughout the system provides the traditional services of integrity, confidentiality, non-repudiation, access control, and authentication. The DMS Security Policy dictates that all organizational messages will be signed and encrypted within DMS, automatically providing authenticity, non-repudiation and integrity (via signature), and confidentiality and access control (via encryption).

4. Interoperability Services (IS)

DMS interacts with legacy users via a Multi-Function Interpreter (MFI) and interacts with other e-mail systems via an SMTP gateway at the groupware server. The MFI is the only component that allows messages to be exchanged between

legacy users (JANAP 128) users and DMS users. Infrastructure MFIs are placed at the National Gateway Center.

In addition to the primary architectural elements, the DMS backbone infrastructure operates in conjunction with the existing Defense Information Systems Network (DISN). The DMS architecture provides a framework for a Service/Agency implementation and a managed backbone infrastructure to plug into. The architecture does not limit an organization to design in terms of a "site," referring to a specific geographic location. It is largely distinguished by its role in the DISN, which participates in the underlying network transport infrastructure. DISN also provides a Simple Mail Transfer Protocol (SMTP) base with which DMS will coexist. The backbone infrastructure topology and a functional view of the DMS architecture are illustrated in Figure 4.

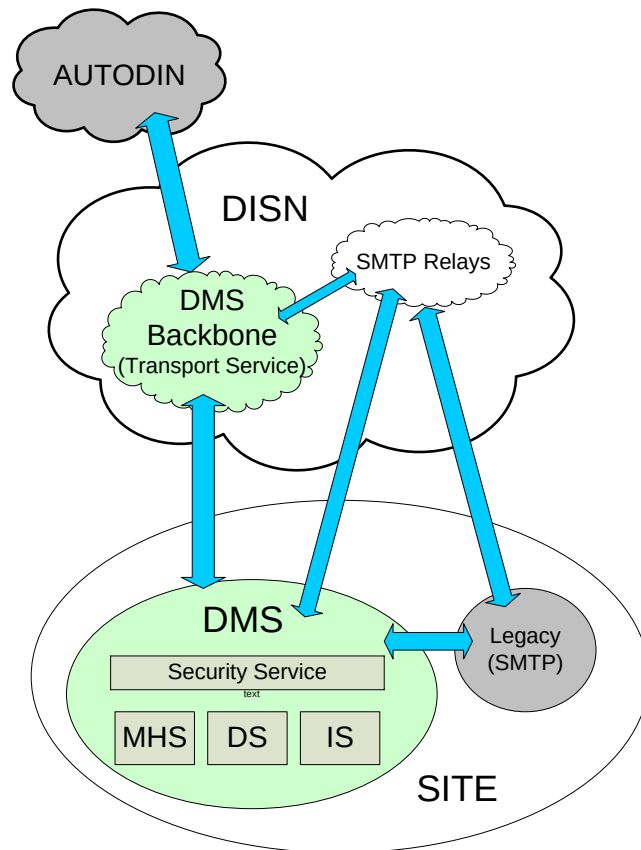


Figure 4. DMS Architecture (Functional View)

B. NREMS ARCHITECTURE ANALYSIS

DMS will evolve from a user agent (UA)-client to the internet explorer (IE)-client for messaging with the AMHS and will cause a significant change in command level business processes. OSD mandated the way ahead for DMS Expanded Boundary Solution-Navy (DEBS-N) approach that will consist of centralized messaging and FORTEZZA security services using a domain FORTEZZA approach. Fundamentally, the overall DMS architecture at the backbone level will remain the same, although consolidation is expected over time (SPAWAR 2006). The most significant change will be at the DMS site level. The NREMS server will replace the dedicated DMS Exchange server at the DMS Service Provider (DSP) and the UA will not be required. To conduct

messaging, customers will use their desktop web browser and DOD Public Key Infrastructure (PKI) credentials. FORTEZZA credentials will remain with the AMHS. The AMHS is comprised primarily of two independent programs running on the same computer. During DMS functions, the programs become interdependent (SPAWAR 2004).

1. CommPower CP-XP

A software application on the AMHS computer that interacts internally with the FORTEZZA card to decrypt incoming DMS traffic or to sign and encrypt outbound DMS traffic.

Externally, the CP-XP application communicates (via the X.400 protocol) the P1 formatted DMS message to and from Message Transfer Agent (MTAs) either in the DISA DMS backbone or with other AMHSs.

Internally, for inbound or outbound processes, the CP-XP interacts with the AMHS via the Extensible Markup Language¹⁵ (XML) standard. Communication is in the "clear" (not encrypted during transit), but the XML in the clear is strictly internal to the computer, therefore it does not transverse an environment subject to compromise, such as a local area network (LAN).

2. Telos AMHS

A software application for the actual AMHS component. The code uses commercial-off-the-shelf (COTS) utilities to achieve its purpose:

- user interfaces with the AMHS computer's Microsoft Internet Information Services (MS IIS) web interface, and

¹⁵ Extensible Markup Language (XML) is a general-purpose markup language. Its primary purpose is to facilitate the sharing of data across different information systems, particularly via the Internet.

- DMS messages are stored on the AMHS computer using the Verity database manager application.

The AMHS concept centralizes the storage and access method for DOD messaging. This is a completely new concept compared with the current distributed messaging system. User's access will be granted via web browser rather than Microsoft Outlook and the administrative and maintenance burden will shift to regional sites. This should greatly minimize the need for messaging support personnel at individual commands (see Figure 5).

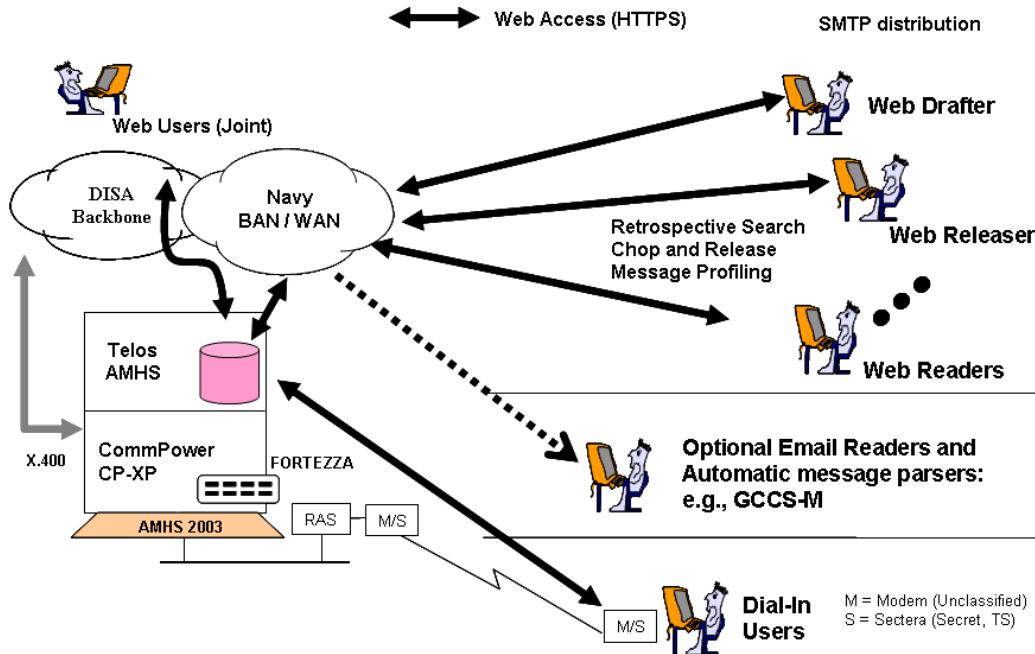


Figure 5. NREMS Architecture (Operational View) (From: PEO C4I 2005)

C. QUALITY ATTRIBUTES

Despite the abundance of DMS literature, explicit mention of the architectures quality attributes were surprisingly absent from the documentation. In absence of expressed quality attributes, the goal then became to focus, using discretion, on the underling areas of quality

interest that seemed to be emphasized the most across the DMS documents that were reviewed. Drawing from the requirements and description of the DMS architecture previously described; several quality attributes emerged implicitly to become relevant for the NREMS evaluation. Security, performance, availability, scalability and maintainability/supportability were determined to be the "highest-priority" quality attributes impacting the requirements described in Chapter III.

Clements et al. defines the following quality attributes chosen for the NREMS analysis.

- Security. Protection of system data against disclosure, modification, or destruction. Protection of computer systems themselves both technical and administrative.
- Performance. The ability of the system to allocate its computational resources to requests for service in a manner that will satisfy timing requirements; i.e., critical messages.
- Availability/Reliability. The long-term proportion of time the system is working and delivering its services. Availability and reliability are closely related.
- Scalability. The ability of a system to support the desired quality of service as load increases without having to change the system.
- Maintainability/Supportability. Maintainability is the efficiency and ease of monitoring and maintaining the system in order to keep the system performing, secure and running smoothly. Supportability is the effective means to keep the system running after deployment based on resources including both knowledgeable and available technical staff. Successful maintenance requires support.

Quality requirements can be categorized as either development or operational. Development quality

requirements are qualities of the system that are relevant from an engineering perspective, such as maintainability. Operational quality requirements are qualities of the system, such as performance and reliability (Bosch 2000 p. 27).

Throughout the quality attribute analysis performance will be referenced often. This is due to the impact various attributes may have on a systems overall operation. For example, the level of confidentiality required in a virtual private network might be sensitive to the number of bits chosen for encryption. In this case, confidentiality would be a sensitivity point and an architect may have to trade-off a performance characteristic such as increased latency to ensure that confidentiality is maintained. At every decision point architects are faced with vices such as these this analysis sensitivity and trade-off points will be further explained throughout the thesis.

1. Security

Security is an essential quality attribute of most DOD systems but there has always been a particular focus in reference to communications systems. The MROC 3-88 specifically addresses three DMS security requirements that must carry-over to NREMS in order to ensure the security of the networked system; specifically, confidentiality, integrity, and authentication. Confidentiality refers to keeping the data private, so only authorized users can view it. Integrity means ensuring that measures are taken so the data cannot be changed, unless by an authorized user.

All DoD Services are migrating to the domain FORTEZZA approach, which is endorsed by the Office of the Secretary of Defense (OSD) and DISA as the way ahead for DMS (SPAWAR

2004). NREMS will employ the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-1 and NSA Certified DMS approved product, Type 2 Cryptographic Support Server (T2CSS). T2CSS incorporates virtual tokens (FORTEZZA, PKI or other Certificate) in hardware providing Class 4 level of assurance¹⁶ (LOA) and the flexibility, scalability and security convenience only possible with virtual tokens. The product supports data confidentiality, data integrity, key management, digital signature and time-stamp services through the use of flexible hardware architecture. The architecture design includes:

1. A multiple cryptographic processor design optimized for a significant performance increase.
2. Scaleable and flexible design - one or more cryptographic processors per board and multiple boards in a system.
3. FORTEZZA Cryptographic Interface (CI) and Application Programming Interface (API) support.

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. The U.S. Government's National Information Assurance Glossary defines strong authentication as: layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information. The NIPRNet will have a DOD PKI server certificate installed that will be used to establish a SSL (128 bit encryption) connection between the user's browser and the AMHS (see Figure 6). The PKI distinguished

¹⁶ The extent to which an electronic identity credential may be trusted to actually represent that the individual named in the credential is the same person engaging in the electronic transaction with the application, service or relying party. Class 4 (Federal High) suggest medium assurance with hardware.

www.cio.gov/fbca/presentations/altermann-terena.ppt, last accessed May 2007.

name will then be associated to the users account, and subsequently, users will authenticate using their CAC certificate and CAC PIN, successfully meeting the NIST required authentication level. The following steps are provided for NIPRNet:

1. Initial login, the user will be required to enter their AMHS user name and password.
2. Select a PKI certificate (CAC identity certificate) and enter CAC Personal Identification Number (PIN) used on the local workstation to unlock access to their private key information on the CAC itself.

SIPRNet Web users will be required to authenticate using a user name and password that will be sent over an SSL session from the user's workstation to NREMS due to the lack of DOD PKI within the domain (see Figure 7). SIPRNet will use the SQL server mode of authentication.

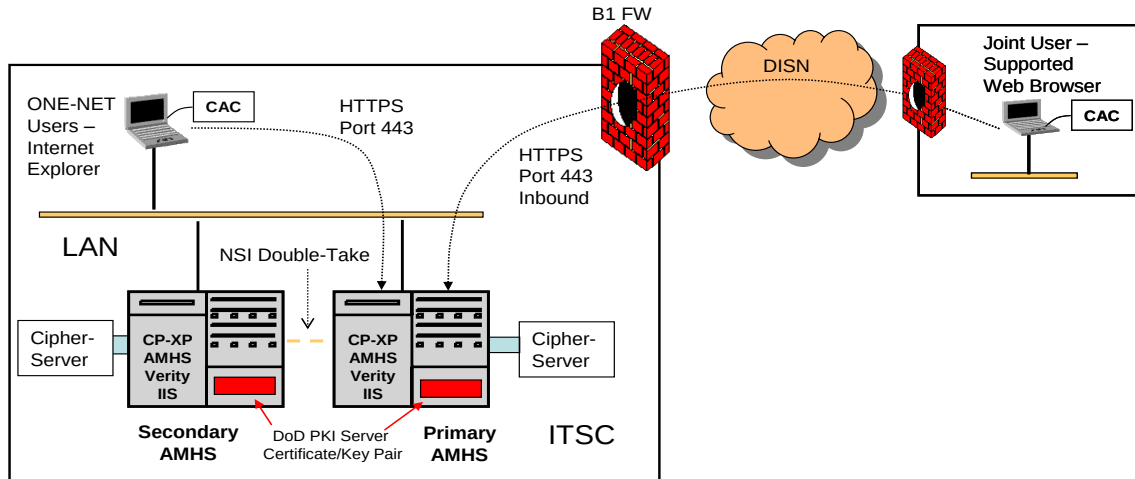


Figure 6. End User Web Access (NIPR) (From: PEO C4I 2007)

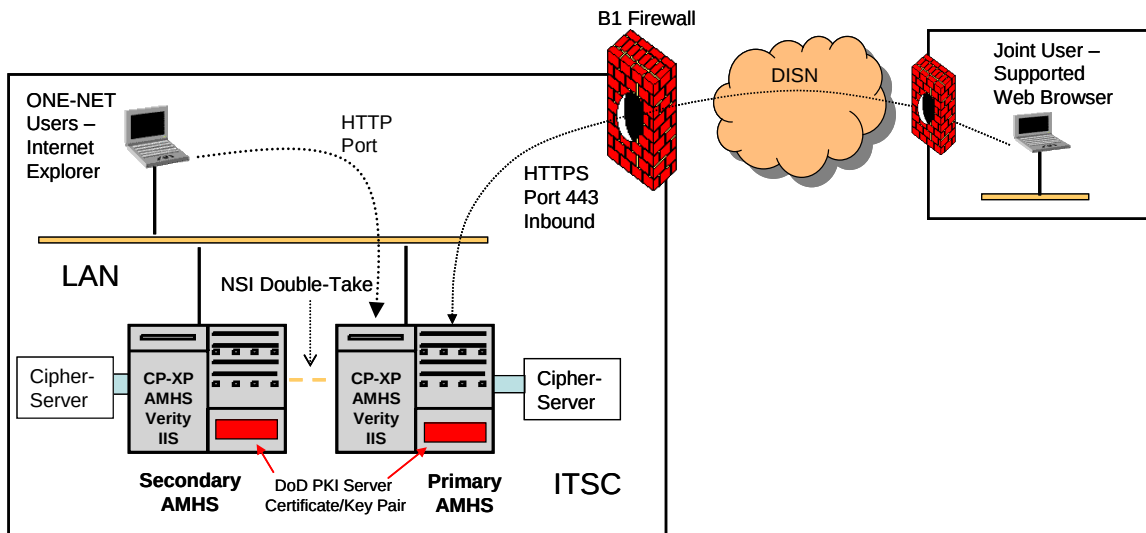


Figure 7. End User Web Access (SIPR) (From: PEO C4I 2007)

Security in information systems is not a simple problem to resolve. Single solutions are often if ever found to meet complex systems requirements. The ISO Reference Model describes seven layers to define service levels. The model is an ideal means to match requirements with solutions (see Table 2). A security rule of thumb states: the higher the layer at which you can gain appropriate security service, the less you have to depend

on the network to provide the service (Class Notes, CC4221; 2002). It is important to note that NREMS successfully implements security protection at all five of the seven layers of the OSI Reference Model with the use of SSL, passwords, and the hardware FORTEZZA solution.

ISO RM Layer	Buzz	Problem	Solution	Examples
7, Application	Secure the data	Confidentiality Authenticity	Object Level Security	S/Mime, SSH, SSL VPN
3-4 Network and Transport	Secure the network/box not the data	Perimeter protection of enclave. Prevent Denial of Service (DOS) attacks	Firewalls, intrusion detection	passwords
1-2 Physical and Data Link	Protect the pipe	Traffic analysis Jammability Detectibility	Link crypto LPI/LPD spread spectrum	KG-84 STU- III

Table 2. OSI Reference Model Organization Matrix (CC4221 Notes 2002)

2. Modeling Quality Attributes

Arena Student Version Modeling software was used to layout the NREMS architecture from the web client to network output. Due to shortcomings in the student version of Arena, modeling hundreds of messages from a total of 30,000 clients is not possible. To work around this issue, clients have been reduced to a total of 700 users, four different message types [large, medium, small message (HTTPS 443)¹⁷ and administrative (SMTP)¹⁸ requests], and

¹⁷ HTTPS URL indicates that Hypertext Transfer Protocol is to be used, but with a different default TCP port (443) and an additional encryption/authentication layer between the HTTP and TCP. <http://en.wikipedia.org/wiki/HTTPS>, last accessed December 2006.

increased the processing time from seconds to minutes. Figure 8 illustrates the portion of the messaging architecture that was modeled, specifically leaving out DMS and legacy systems interconnected.

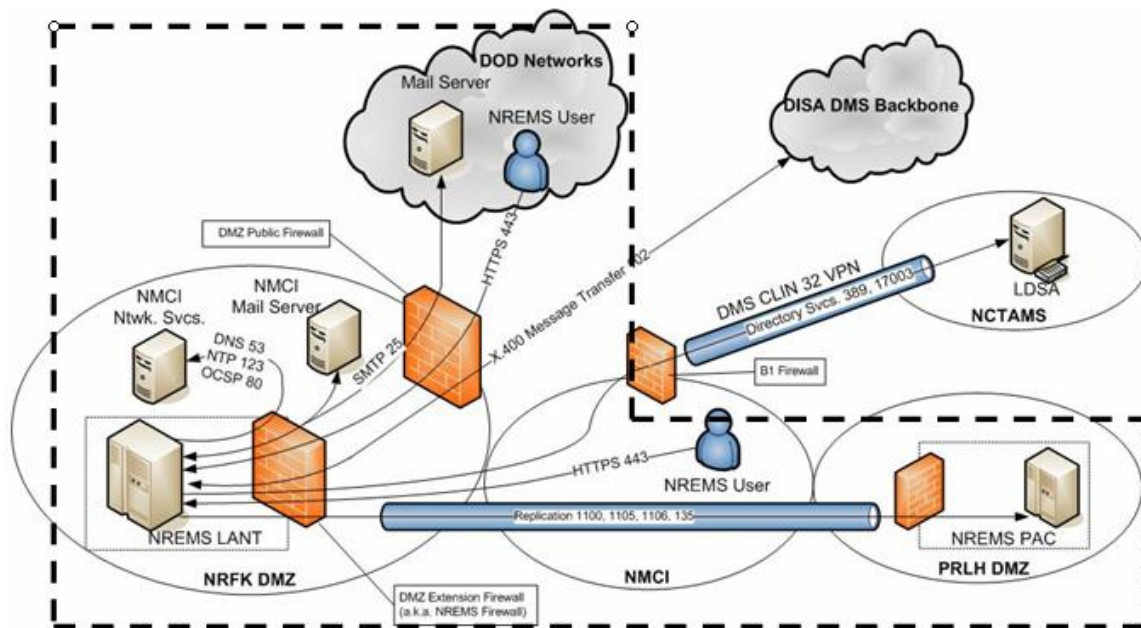


Figure 8. Arena Network Components Model (From: PEO C4I 2005)

The goal of the model is to compare the average wait time, total time in the system and the total number of released messages, during points of traffic surge or network failure. In engineering terms this scenario is defined as message latency; the time delay between the moment something is initiated, and the moment one of its effects begins or can be detected. Latency tends to be inversely proportional to the performance of QoS of a system.

¹⁸ Simple Mail Transfer Protocol (SMTP) is the de facto standard for e-mail transmissions across the Internet. <http://en.wikipedia.org/wiki/SMTP>, last accessed December 2006.

Modeling methodology centered on building a symmetric messaging architecture processing only inbound SMTP and HTTPS 443 traffic of varying size lengths and types. Following entity creation, each message will transit through the Navy Marine Corps Intranet (NMCI) OC-3¹⁹ fiber optic pipe onto the NREMS network, specifically through the following dedicated components:

- Domain Controllers - used for policy, security, and authentication
- AMHS - System profiler - Incoming feed for web-based system
- CP-XP /w T2CSS - gateway to DMS network (DMS component)
- IIS Web Server - provides the web interface for AMHS
- SQL - the database server keeps a record of all messages, users, and the message access granted to those users
- Autonomy K2 - performs retrospective search function
- Storage Area Network (SAN) - message store (12-24 Terabytes)

Each dedicated component exists in pairs of two for a total of four components, two primary and two Continuity of Operations (COOP), in each regional site with the exception of the IIS. Each component has a dedicated process with a triangulation distribution process time between 0.5 to 1.5 minutes of process time. Each entity (message) is processed at the primary system then duplicated to be stored in the COOP. The following four scenarios will be modeled using 20 replications:

¹⁹ OC-3 is a network line with transmission speeds of up to 155.52 Mbit/s (payload: 148.608 Mbit/s; overhead: 6.912 Mbit/s, including path overhead) using fiber optics. <http://en.wikipedia.org/wiki/OC-3>, last accessed March 2007.

- Scenario 1: Failover
- Scenario 2: AMHS Server Quantity Variations
- Scenario 3: Peacetime vs. Wartime Surge
- Scenario 4: Wartime Surge and Failover

Using a set baseline derived from a scenario situation with all dependent variables constant, an approximation was obtained of each scenario effects on the entity time parameters, specifically time in system and time to process. Figure 9 illustrates the model for the NREMS NCTAMS Pacific architecture. The model also includes the NREMS NCTAMS LANT architecture (not illustrated) which is interconnected to the NREMS NCTAMS PAC model to simulate failover.

Each model includes the NREMS primary and COOP site, with the same number of servers per dedicated component. Additionally, message creation modules allow the alteration of inter-arrival times for each message type and administrative request. The manipulation (shortening or lengthening) of the inter-arrival times will allow the model to simulate surge periods based upon the time of day and wartime time periods.

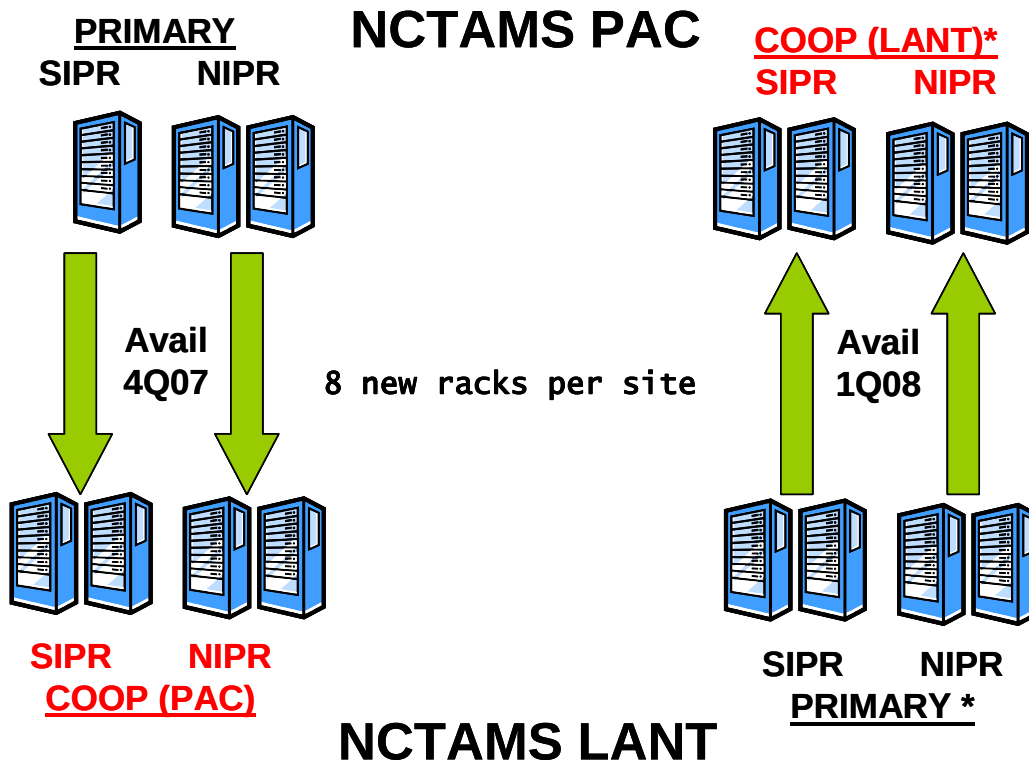


Figure 10. NREMS High Level COOP Diagram (From: PEO C4I 2007)

As the basis of this analysis NCTAMS PAC and NCTAMS LANT connectivity will be mapped to assess system performance under different scenarios (see Figure 11). In one embodiment of a model, NREMS availability and reliability will be determined based upon varying the following parameters:

1. Number of incoming messages and administrative requests
2. Message type:
 - a. Large Message: Message length > 4Kbytes
 - b. Medium Message: Message length between 512bytes and 4Kbytes
 - c. Small Message: Message length < 512bytes
3. Message pipe failure on PAC or LANT NREMS network

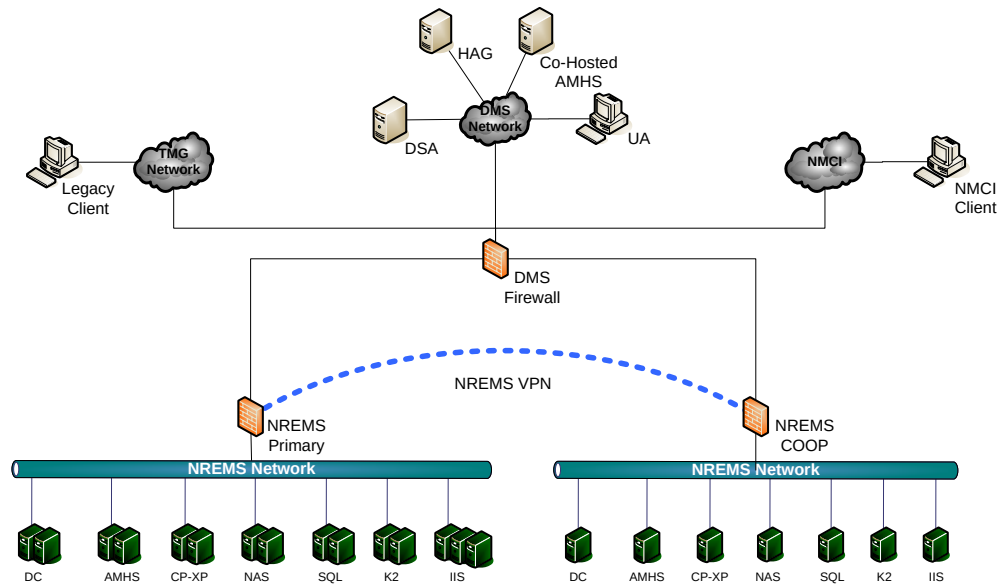


Figure 11. NREMS Logical Diagram (From: PEO C4I 2007)

As alluded to earlier, sensitivity points are parameters in the architecture to which some measurable quality attribute response is highly correlated. A tradeoff point is found in the architecture when an AMHS server is host to more than one sensitivity point where the measurable quality attributes are affected differently by changing a particular parameter. In the following analysis, there are two sensitivity points measured in relation to overall system availability and reliability: total time within the system (NREMS) and the total number of messages processed.

3. Maintainability/Supportability

The two RNOSC NREMS implementation is the Navy's attempt to re-architect the unsuccessful implementation of the DMS project by resolving labor-intensive installations, operations and maintenance issues. The program boasts of substantial costs savings over the next 10 years for the Navy, particularly to the end user commands, by alleviating the command's FORTEZZA and client workstation requirements

and reducing personnel necessary to operate and maintain the equipment (PEO C4I 2005). The centralization of the core functions of the messaging systems will significantly decrease the need for command level expertise in functions such as upgrades, updates, simple and complex level maintenance, and troubleshooting for the system. Field Engineering Notices (FENs) such as Figure 12 often over burden units to keep each component of the DMS system within the required guidelines for security and version control.

Microsoft Outlook 2003 DMS Client Availability
FEN 3.1.3-OUTLOOK2003-CD-02A
The DMS 3.1.3-Client (FEN 3.1.3-OUTLOOK2003-CD-02A) is now available on the Naval Messaging Web site. To order the FEN and executable, go to <https://navalmessaging.spawar.navy.mil/>. Select DMS 3.1 Transition.

Audience
The purpose of this MANDATORY FEN is for the installation of the Outlook 2003 DMS client on Windows XP. The intended audience for this FEN is DMS Administrators. The installer should have knowledge of Microsoft Windows XP functionality and operating system commands.

Timeframe
All commands must complete their upgrade by 30 June 07. Failure to meet this requirement could result in a service disruption and may preclude proper DMS operations.

Summary
The following install paths are supported in this FEN:

- New installs on Windows XP
- Up  from Outlook 2002 DMS Version 3.0.4.0 or higher on Windows XP
- Up  from commercial Outlook 2002 on Windows XP

Required Actions
The upgrade path requires the Windows XP operating system. A backup of the DMS database manager, PST files, PAB and anything else deemed important is highly recommended. Should problems arise from the installation the backup can be restored.

Dependencies
The Outlook 2002 client should be at 3.0.41.0 or higher on Windows XP.

Assistance
Please contact the Navy Global DMS Consolidated Help Desk (DCHD) @ 877-646-1476 or (dsn) 646-9997 opt 1.

Figure 12. DMS Field Engineering Notification (FEN) (From: Email: TSA 2007)

The maintenance and support burden of the system will be eased by the 2 RNOSC concept and the procurement plan for the system. Approved products will be provided 24/7 support with a contract vehicle in place for system upgrades. The burden will shift from individual DSP sites to the designated RNOSC whom will be designated the responsibility for all of the complex maintenance and upkeep functions such as FEN updates, AMHS backups, FORTEZZA, and command level account established. This will leave minimal responsibilities to the local command. System Administrators will be held responsible for establishing local user accounts via a web based process.

D. SCENARIOS

1. Scenario 1: Failover

Failover is defined as the capability for a system to switch over automatically to a redundant or standby computer server upon the failure or abnormal termination of the previously active server. The NREMS architecture has the capability to switchover to the assigned alternate regional site. The following scenario will evaluate NREMS redundancy amidst primary and COOP site failover and how data consistency is maintained (so that one component can take over from another and be sure that it is in a consistent state with the failed component).

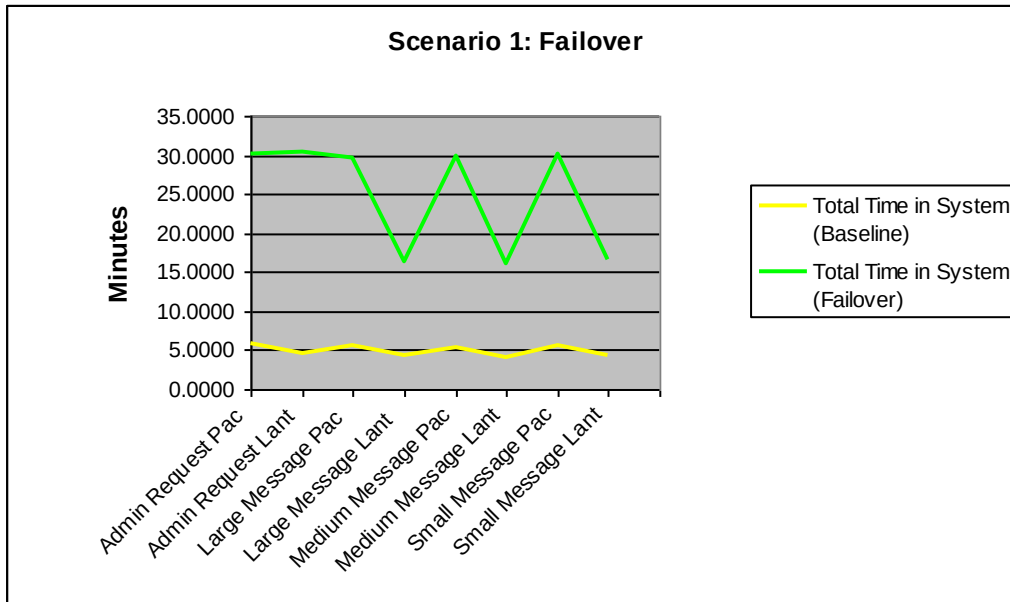


Figure 13. Scenario 1 Failover Total Time in System

In this particular scenario, NCTAMS PAC fails and NCTAMS LANT site must perform dual network operations (primary and COOP services), handling the messages and administrative requests transmitted during normal network operations for both sites. Over an eight-hour normal workday, the average total time in system for 70% of the messages transmitted was six times longer than normal operations. This six-fold increase in total time in system results in a 33% reduction in released messages (i.e., messages outbound from NREMS network to DMS backbone). The increased number of messages decreases the systems performance; specifically, the trade-off for increased message volume is an increase in processing time, resulting in decreased system performance.

2. Scenario 2: AMHS Server Quantity Variation

Prior to delving into this scenario, it is important to explain the reason for the emphasis on the AMHS servers of the NREMS architecture. The AMHS is designed as a

network solution to alleviate the problems faced by organizations with large volumes of message traffic sent to and from generic email services. The AMHS allows the organization's users to filter and route messages based on context, preference, and priority. The AMHS solution also provides support for the DOD's AUTODIN and DMS messaging systems, making it available to the legacy and DMS architectures as individual commands migrate systems. Since the AMHS servers play such an intricate role in the entire NREMS network, a majority of the time constraints in the model are considered based on the AMHS server ability to adapt to both physical and logical changes in the system.

Scalability is the ability of the AMHS to shrink and expand to fulfill existing and future system requirements. This attribute is essential to the overall performance, availability and reliability of a system. For the purpose of this thesis, the AMHS servers were physically expanded to make use of 3 servers vice 1. The model architecture variability tests the effects of an increased capacity on the systems available resource usage distribution. The Arena-modeled variability in the server architecture from 1 to 3 resulted in a minimal increase in overall systems efficiency which may prove to be much smaller than the increased costs and maintenance associated with the architectural change.

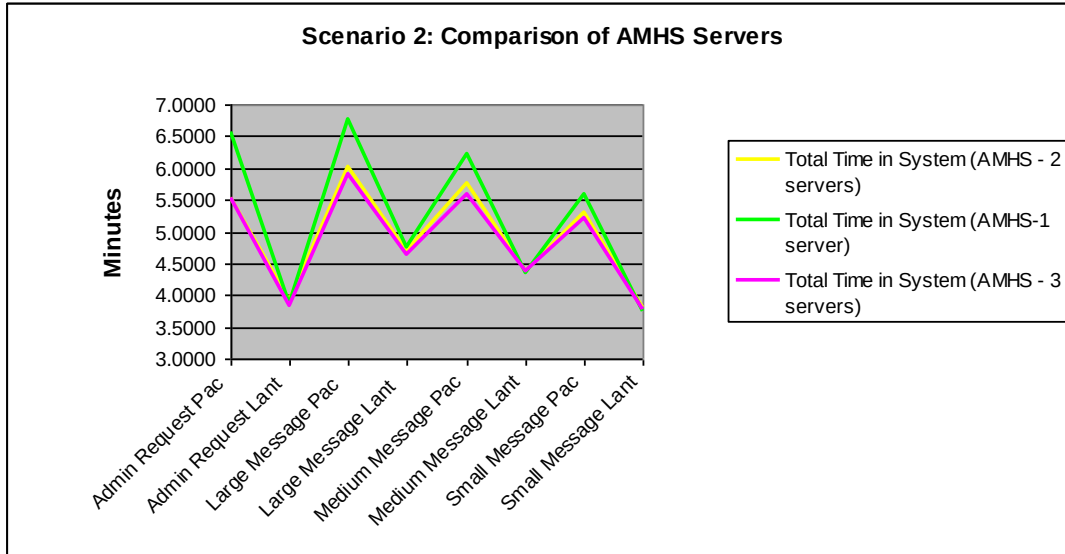


Figure 14. Scenario 2 AMHS Server Quantity Variation

3. Scenario 3: Peace Time vs. Wartime Surge

Wartime surge capability is modeled by varying the message and administrative request inter-arrival times to half the baseline value.

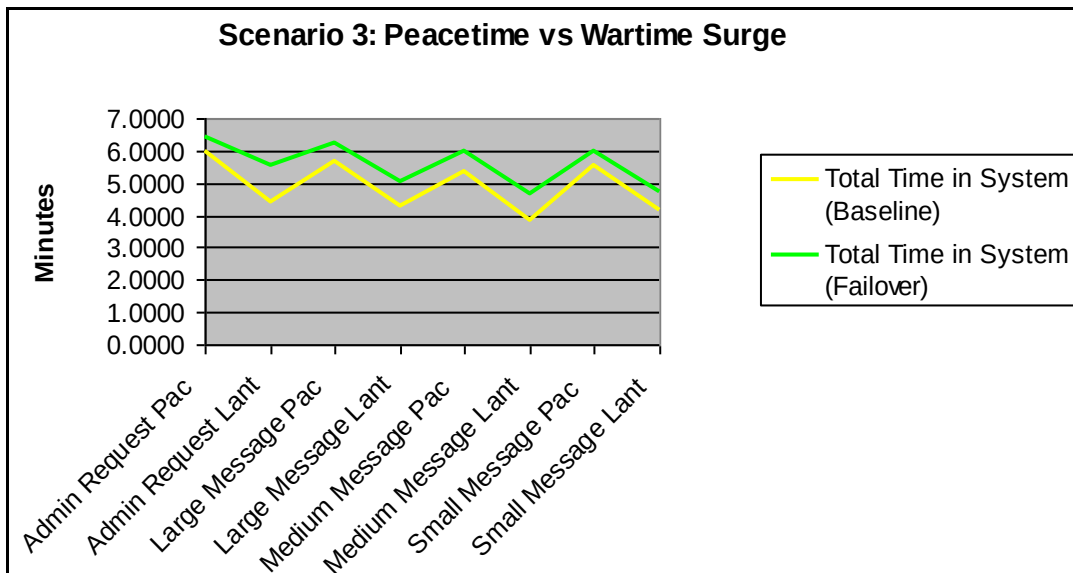


Figure 15. Scenario 3 Peacetime vs. Wartime Surge Total Time in System

During normal and wartime simulations, 556 and 1,732 messages and administrative request were transmitted

respectively. The difference in total time in system for each message type from a peacetime to wartime scenario is minimal (approximately a 15% increase in total time in system).

4. Scenario 4: Wartime Surge and Failover

The following scenario will evaluate NREMS redundancy amidst failover and availability during a wartime surge period. The failover consists of a failure on the NCTAMS PAC network, causing all messages from the Pacific coast to utilize the NCTAMS LANT network to process all messages and administrative requests. The wartime surge scenario is modeled by cutting in half the inert-arrival times of each message transmission and administrative requests.

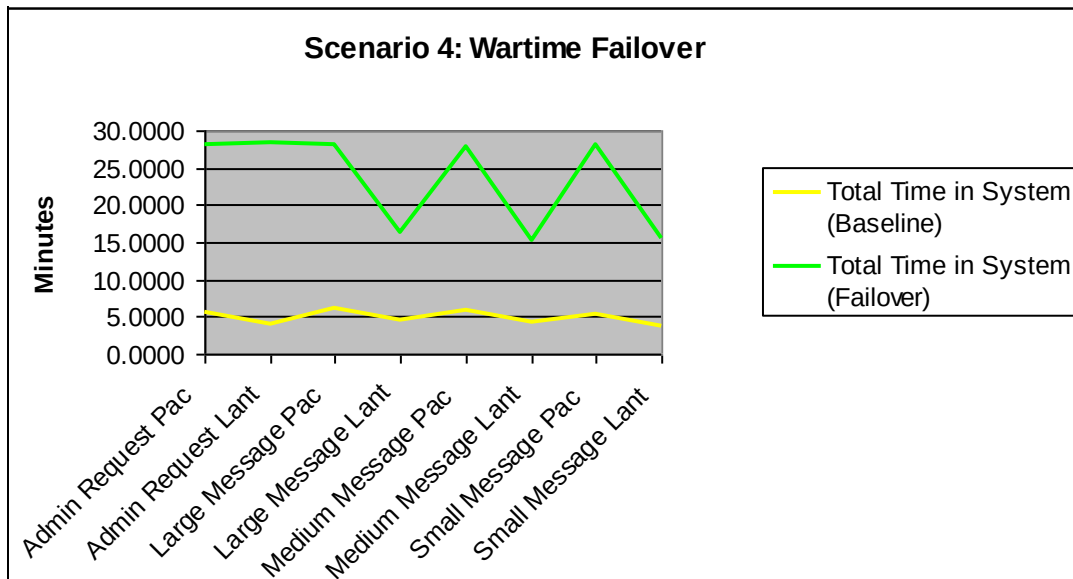


Figure 16. Scenario 4 Wartime Failover Total Time in System

During normal and wartime simulations, 524 and 722 messages and administrative request were transmitted respectively. Over an eight-hour normal workday, the average total time in system for 50% of the messages

transmitted was six times longer than normal operations. This six-fold increase in total time in system results in a 33% reduction in released messages (i.e., messages outbound from NREMS network to DMS backbone).

E. USER SURVEYS

Little data exists to characterize existing Naval messaging business processes or to determine the best, future business process to implement for an organization. How many Naval messaging organizations currently use a DMDS? How many message readers, drafters, and releasers does each organization have assigned? How often do organizations access messaging resources? When do they access messaging most? This data is required to determine what business processes and resources should be in place after the transition from DMS to NREMS in order to adequately support the needs of Naval messaging.

In conjunction with the Space and Naval Warfare Systems Command, San Diego, a decision tree was developed to assist the NMWG and Naval messaging organizations with how to best structure their assets after the transition from DMS to NREMS. (see Figure 3) Past survey efforts have consisted of requests, via formal Naval messages, for organizational data from Naval messaging organizations. These requests have received little if any response using this method. Instead, a web-enabled survey was developed with questions that were easy to answer (point and click). The entire survey requires less than ten minutes to complete. The data gathered will be used to navigate the decision tree developed and determine which business process each messaging organization should implement. Additional areas of interest to the Space and Naval Warfare

Systems Command were also added to take full advantage of the opportunity to reach Naval messaging organizations, i.e., questions not required to navigate the decision tree but would assist in determining when and how to deploy messaging assets.

1. NREMS Business Processes

Within NREMS, the NMWG has defined six separate business processes that each Naval messaging command can adopt as appropriate. Each business process is defined by outbound messaging requirements and inbound messaging requirements.

For outbound messaging, messages can be released either using a web proxy or an SMTP proxy. A web proxy requires no resources at the command level other than a computer with a web browser. An SMTP proxy requires setup at the command and command resources to maintain. SMTP proxies are required for commands that have a large number of outgoing message traffic.

For inbound messaging, messages can be received either directly through the internet (web interface) or through the use of a DMDS. Again, web users require no resources at the command level other than a computer with a web browser. A DMDS requires setup at the command and command resources to maintain. A DMDS is required for commands that have a large number of inbound message traffic.

The six business processes are variations of outbound messaging requirements (web vs. SMTP) and inbound messaging requirements (web vs. DMDS). These business processes are as follows:

- Outbound: SMTP Proxy
Inbound: DMDS Folder Delivery
- Outbound: SMTP Proxy
Inbound: DMDS User Delivery
- Outbound: Web Proxy
Inbound: DMDS Folder Delivery
- Outbound: Web Proxy
Inbound: DMDS User Delivery
- Outbound: Web Proxy
Inbound: Web Bulletin Board Delivery
- Outbound: Web Proxy
Inbound: Web User Delivery

The business process assigned is based solely on four organizational characteristics: number of message releasers, number of message drafters, number of message readers, and the use of read boards or public folders. By responding to questions about these characteristics, a Naval messaging organization can determine which model best fits their command messaging requirements. By gathering data about these characteristics, the Space and Naval Warfare Systems Command can determine how to best allocate resources for customers that might require a DMDS or SMTP proxy.

2. The Survey

a. Survey Terminology

Concurrent searches: Readers performing a search of messages simultaneously; an important attribute that must be monitored to maintain an appropriate NREMS load.

Message Drafter: Those individuals with the authority to draft messages within AMHS.

Message Reader: The majority of NREMS users; those individuals with the authority to read messages within AMHS.

Message Releaser: Those individuals with the authority to release a message from their organization to another organization.

Messaging rush hour: The period of time during a normal workday when message readers will typically access messages and messaging resources. Normally, this occurs at the beginning or end of a work day.

PLA: Plain language address. A unique identifier used by Naval messaging organizations similar to a mailing address. Used to identify the sending organization on the "FROM:" line or the intended receiving organization on the "TO:" line of a Naval message. For example, the PLA "AIMD WHIDBEY ISLAND WA" indicates Aircraft Intermediate Maintenance Department, Whidbey Island, Washington.

Read board or public folders: equivalent terms referring to the method of message delivery. Messages can be delivered to specific individuals via email or to a read board/public folder that readers can access.

Search of messages: The ability to search for key words in current messages or the messaging archive. DMS does not offer a search engine for current or archived messages. NREMS will offer this feature. However, care must be taken to monitor the NREMS load while conducting searches as searches require a significant amount of system bandwidth.

Zulu Time: Greenwich Mean Time; Universal Coordinated Time (UTC).

b. Survey Development

Survey questions were carefully crafted to navigate the Naval messaging business process decision tree for NREMS and to gather additional information of interest to the NMWG. The survey questions were submitted to the NMWG and its members for review and approval. Once approved, the final survey was drafted utilizing the tools available in the website SurveyMonkey.com.

SurveyMonkey.com was selected as the data gathering mechanism for the survey. This website contains easy to use survey templates that gather information, store it, and publish it to the researcher in a multitude of useful formats: spreadsheet, HTML (web pages) and Adobe Acrobat files (.pdf).

A draft survey, utilizing the approved survey questions, was created in SurveyMonkey.com. A web link was created to the survey and disseminated to members of the NMWG via email. Interested parties were given one week to view and navigate the survey and provide feedback. The feedback was addressed either by provision of additional clarifying information or revision of the survey and the final survey was agreed upon. Then, a web link was created to access the final survey and ready it for dissemination to all registered Naval messaging users.

c. Survey Dissemination

The web link to the survey was disseminated to every registered Naval messaging user via email. (See Figure 2) All Naval messaging users are required to register with the Naval messaging website. On the date of

survey delivery to prospective respondents, the Naval messaging website had 1,659 registered users. The web link to the survey was emailed to all 1,659 registered users.

Our target population was all command system administrators. Each system administrator is responsible for managing access to the Naval messaging resources for their command. Command system administrators add and delete message releasers, drafters and readers and develop and enforce local Naval messaging policies. Command system administrators are responsible for maintaining all command hardware and software in support of Naval messaging. Only one response was required per command (PLA) and only from the command system administrator who is most qualified to provide it.

Once the email was released, command system administrators were afforded two weeks to complete the survey. At the end of the two weeks, the survey was closed and could no longer be accessed. On the date of survey delivery, the Space and Naval Warfare Systems Command estimated the number of command system administrators to be 850. We received 178 responses from our target audience of 850.

3. User Survey Analysis

Once the survey was released, the data was gathered in real time as respondents accessed the web link. After the survey was closed, the data was reviewed for completeness and incomplete data was deleted. The remaining data was imported into a Microsoft Access database. Queries and reports were generated in Access to determine the appropriate business process for each responding

organization and then extrapolated across the Naval messaging enterprise. All data and analysis were provided to the thesis sponsor.

a. Data Gathering

As each respondent (command system administrator) accessed the web link, they were directed to the first page of the survey, the informed consent page. (See Appendix A) Once respondents agreed to the conditions of the survey, the respondents could access the survey questions. The survey maximized the use of radial buttons (one answer only) and required responses to the survey questions that were necessary to navigate the Naval messaging business process decision tree. Respondents could also exit the survey at any point and return to the survey later if desired.

The survey responses were stored in real time in a database by SurveyMonkey.com. Researchers could access the results at any time during the survey to monitor progress. Some survey responses were deleted entirely if insufficient information was gathered to navigate the decision tree. The majority of deleted responses included nothing beyond agreeing to the informed consent page and provided no useful information. Approximately 50 responses fell into this category.

At the end of the survey period (two weeks), the survey was closed and the data exported into a Microsoft Excel spreadsheet. The Excel spreadsheet was reconfigured so that it could easily be imported into Microsoft Access. The resulting Microsoft Access database table can be viewed in Appendix B.

Not all data gathered were imported into Access as not all data was required to navigate the decision tree. However, the complete set of data in an excel spreadsheet was maintained and forwarded to the thesis sponsor, the Space and Naval Warfare Systems Command. An overview of the data gathered, as provided by SurveyMonkey.com, can be viewed in Appendix C.

b. Data Analysis

Using the Naval messaging business process decision tree (Figure 3), eight queries were written in Microsoft Access to determine which and how many commands fit into each Naval messaging business process. Two of the end nodes can be reached using two separate paths depending on the respondent's answer to survey question number three: "How many message releasers does your organization have?" Therefore, two additional queries were required to reach each of these two end nodes. Appendix D contains the SQL queries.

Using the queries, eight reports for each of the six business processes were designed to list each PLA for each business process type as well as the total count. Appendix E contains the generated reports based on the data gathered.

Table 3 contains the summary of the data gathered. Each of the 178 respondents was characterized by using their responses to navigate the decision tree. Of the 178 responses, 11 respondents did not provide enough information to navigate the tree and were labeled as unknown business process model. However, only six percent of responses fell into this category. Three additional responses were considered suspect: one PLA was listed twice

with conflicting information and another PLA was listed as “we guard for over 100 PLA’s.” After discussions with the Space and Naval Warfare Systems Command, those three responses were left in the data as it was believed that they would not skew the data sufficiently to be of concern.

	Business Process	Business Process	Business Process
	Model Count	Model Percentages for Sample Size	Model Count for Population Size
Outbound: SMTP Proxy Inbound: DMDS Folder Delivery (< 20 Releasers)	15	8%	72
Outbound: SMTP Proxy Inbound: DMDS Folder Delivery (> 20 Releasers)	14	8%	67
Outbound: SMTP Proxy Inbound: DMDS User Delivery (< 20 Releasers)	4	2%	19
Outbound: SMTP Proxy Inbound: DMDS User Delivery (>20 Releasers)	7	4%	33
Outbound: Web Proxy Inbound: DMDS Folder Delivery	36	20%	172
Outbound: Web Proxy Inbound: DMDS User Delivery	22	12%	105
Outbound: Web Proxy Inbound: Web Bulletin Board Delivery	24	13%	115
Outbound: Web Proxy Inbound: Web User Delivery	45	25%	215
Unknown	11	6%	53
Total number of Respondents (Sample Size)	178	100%	850
Population Size	850		
	98	55%	468
Inbound: DMDS Users	69	39%	329
Inbound: Web Users	167	94%	797
Total			
Outbound: SMTP Proxy	40	22%	191
Outbound: Web Proxy	127	71%	606
Total	167	94%	797
Current DMDS Users	115	65%	468

Table 3. Summary of Data from User Surveys

Although we attempted to gain responses from our total population of 850 messaging commands, our sample population consisted of 178 messaging commands (those that responded with sufficient information to navigate the decision tree). We received responses from 20.9% of our total population. We do not have enough information to determine if our sample adequately represents the total

population. We are unaware of an unusual number of responses from any one category of messaging command that might skew the data in any direction. Therefore, it is assumed that the data gathered does not unduly represent any specific category of messaging command, but adequately represents all of Naval messaging.

c. Data Provided

A copy of the entire database with the preformatted queries and reports was provided to our sponsor, the Space and Naval Warfare Systems Command. Data can easily be added, deleted and edited without affecting the queries or reports. The queries can be rerun and revised reports printed from the revised data.

Additionally, a complete copy of all responses were supplied to our sponsor in an excel spreadsheet that can be filtered to focus on data of interest.

VII. CONCLUSIONS

This chapter will summarize the findings of the ATAM, the change management process analysis and the analysis of user surveys. Architectural conclusions will be based upon NREMS ability to meet the OSD and JCS requirements for organizational messaging (interoperability, availability, scalability, and maintainability) while maintaining an acceptable level of security risk. Chapter VI quality attribute and modeling sections will be used to support the author's conclusions. NREMS problem characterization, Chapter IV Section B.3 will be addressed for their potential impact on mandated requirements. Business Process Reengineering (BPR), based upon user surveys, conclusions will provide a basis for the potential success or failure of the NREMS implementation within the Navy. User needs and their level understanding will be the focal points of discussion.

A. ARCHITECTURE FEASIBILITY

Interoperability is the key to achieving net-centric warfare. Information systems within the DOD and among our allies must communicate within a common framework with common definitions of data in order to effectively process information and allow leaders to provide sound decisions.

1. Interoperability

NREMS is a web based system which can be accessed via SMTP, providing an inherently interoperable messaging system. SMTP is a common framework for web-enabled messaging. This creates an environment in which allies can operate with read-only privileges and rely upon their traditional communications systems for transmitting message

traffic. The ability of the AMHS to integrate with other external systems i.e., legacy provides the ability to transmit and receive traffic without degrading the level of service and will appear transparent to the customer.

2. Availability

Availability to a secure web based message search capability with minimal disruption of services is at the discretion of many factors. For the purpose of this thesis the problems characterized within Chapter III; NMCI Connectivity, DOD PKI availability, and CP-XP service restart time will be the focal points of discussion.

a. Navy Marine Corps Intranet (NMCI) Connectivity

Insufficient bandwidth has always been on the Navy's top 10 lists of communications constraints. The Navy Marine Corps Intranet (NMCI) provides the Department of the Navy (DON) with network-based information services on a single, enterprise-wide intranet. NREMS will become a critical operational system within the NMCI environment and therefore must go through the rigorous approval process currently in place. NMCI must be prepared to provide sufficient connectivity, bandwidth and network services to support NREMS. The current state of affairs leaves way for schedule delays, costs increases and potential access control conflicts. The following are examples of ongoing issues:

1. February 2007, SPAWAR 055 Capacity Management Team ordered an OC3 (155.52 Mbps) circuit upgrade at NCTAMS PAC to sufficiently support COOP responsibilities for NCTAMS LANT. The circuit was scheduled to be complete by May 2007, yet it remains an open order with NMCI contractors.

2. Since the OC3 installation was not part of the original contract, the costs associated with the bandwidth upgrades are unknown until the project is complete.
3. Although DISA owns the Global Information Grid (GIG) firewall, the NMCI firewall is controlled by the NMCI contactors. All ports must be approved prior to opening. This problem may seem minuscule, however as stated earlier the approval process within the NMCI network is no easy tasks. The simple addition of applications such as AUTOCAD has been known to take up to two months to be authorized. In the case of NREMS, "ActiveX" must be allowed in order to interact with the AMHS via Internet Explorer. This was not originally approved on NMCI systems; therefore a request was placed to enable this function on the NMCI clients.

b. DOD PKI availability

PKI is not completely established in the unclassified domain, not well established in the SECRET messaging domain and completely lacking in the Top Secret/Collateral (TS/C) messaging domain. Although the high side networks are considered secure networks, PKI ensures authenticity, integrity and confidentiality for DOD messaging is maintained. The absence of PKI does not meet DMS MROC 3-88, NIST or FIPS mandated requirements.

c. CP-XP Service Restart Time

The CP-XP performs a re-caching (or revalidation) service of stored certifications and, based on the quantity of personalities hosted by a particular AMHS server, can be an operation preventing timely and full return-to-service of the AMHS overall. The impact posed by the profilers process shut down is a complete system failure and the activation of failover to the backup system.

3. Scalability

The ability of the system to scale to fit a large-scale enterprise while maintaining all the messaging performance characteristics during peace and wartime operations requires a more in-depth analysis than the Arena data presented within this thesis. The multi-user capability of the AMHS has been tested and approved for a load capacity of up to 30,000 users within a network environment. Although this is a significant accomplishment from the original single service server, the Arena model displays inconsistent performance during increased volumes of traffic (Scenario 3), particularly when the need arises for a single RNOSC to perform dual network operations for both PAC and LANT users.

a. Failover

Arena modeled scenarios 1 and 4 resulted in a six-fold increase in total time to process within the system, or a 33% reduction in the amount of messages released under normal operations. The increased volume of messages decreases the systems performance under the current proposed architecture.

b. AMHS Server Quantity Increase

An attempt to increase the number of AMHS servers resulted in a minimal increase in efficiency for the overall system. Based upon the Arena modeling scenario 2, up to 3 AMHS servers were made available to increase the efficiency of processing increased volumes of messages. The results proved insignificant to increase the performance of the system whether in normal or wartime operations. It appears that there is no value added to increase the number of AHMS servers available for processing messages. The author suspects that this

architecture is unable to use hardware as a viable solution to its load balancing problem because all message traffic must be processed in three different systems.

1. Processed via the primary system.
2. Stored within the local site back-up system for redundancy with the use of "Double-Take²⁰."
3. Shadowed at the alternate COOP site via VPN for contingency purposes.

More hardware may actually complicate this process vice increase performance and efficiency.

4. Maintainability

Maintainability of the system based upon the 2 RNOSC concept significantly decreases costs and increases the standardization and compliance of the DMS architecture. The current DMS architecture poses several significant issues that can be significantly decreased if not alleviated by NREMS; specifically:

1. Costs to support eight DSP sites and command level UA requirements.
2. Dedicated messaging client hardware with a FORTEZZA card at each site to attain security.
3. FORTEZZA card, a token, requires special knowledge by administrators for issuing certificates, creation, storage and handling.
4. End users accountability for the safeguard of the FORTEZZA card upon issue throughout the cards lifespan, this poses various storage and handling issues.
5. Certificate Authorities (CAs) are often off-site and non-local which creates a logistical nightmare during the issuance or re-issue of the FORTEZZA card.

²⁰ Double-Take software products and services enable customers to protect and recover business-critical data and applications to support disaster recovery, high availability and centralized backup. <http://www.doubletake.com/> last accessed 2 May 2007.

6. Maintenance requirements placed on the end user with regards to the DMS client. The client requires regular and sometimes very complex patches or configuration updates.
7. High level DMS administrative skills and often extensive timelines for DMS Service Providers (DSPs) to fully implement the necessary updates.

NREMS or the Telos AMHS has the potential to resolve these costly maintenance and support issues.

5. Summary

NREMS architecture can achieve the requirements of a messaging system as set forth by OSD and JCS. Because NREMS is a web-enabled version of DMS, it remains an interoperable messaging system within DOD and among our allies. Although availability remains an issue with Navy networks, availability is not an issue with NREMS. Bandwidth, PKI and CP-XP performance are easily resolved by procuring available technology. These issues are not issues resulting from the use or implementation of DMS/NREMS, but issues common for naval networks. NREMS is easily scaled for any naval messaging organization. However, NREMS should still be tested as a complete system in a high demand environment. DMS was tested in this manner. The complete NREMS has yet to be tested. Reducing the Naval message stores to two locations and creating a web-enabled system drastically reduces the maintenance requirements of Naval messaging with the implementation of NREMS. With the proper procurement of appropriate technology to support the NREMS product, NREMS is capable of achieving all of the requirements set forth by OSD and JCS.

B. BUSINESS PROCESS REENGINEERING FEASIBILITY

This thesis analyzed the NREMS project implementation plan, surveyed Naval messaging users, and characterized the business processes for Naval messaging organizations after implementation of NREMS.

1. Change Management Analysis

It is apparent from the analysis of the change management process and encounters with Naval messaging users during our research, that some Naval messaging users (change recipients) distrust and are skeptical of the transition from DMS to NREMS. Other users are unaware of the transition.

Naval messaging commands and capabilities suffered greatly during the transition from AUTODIN to DMS. To date, AUTODIN has still not been completely phased out. Culturally, Naval messaging users are unwilling to make another transition, regardless of its viability. Naval messaging users and their perceptions are the biggest roadblock to this change endeavor.

A tremendous effort has gone into providing resources for Naval messaging users regarding NREMS: website, training courses, newsletters, etc. All of these resources exist in a pull format. In other words, interested users must be willing to access the information in order for them to receive it. Because end user buy-in is very low, few people are willing to access these resources. As a result, few individuals are aware of the NREMS project.

2. User Surveys

The data gathered from user surveys is characterized in Table 3 and Appendix C. From that data, we can determine the following (see Table 4):

- DMDS users will decrease by 6% after implementation of NREMS, producing a minor decrease in resources required.
- Naval messaging organizations will receive 41% of their messages and send 76% of their messages through the web portal.
- The majority of Naval messaging commands (76%) have fewer than 20 message drafters and 20 releasers and will function well with a Web proxy for outgoing messages.

Total number of Respondents (Sample Size)	178	100%	850
Population Size	850		
Inbound: DMDS Users	98	59%	468
Inbound: Web Users	69	41%	329
Total	167	100%	797
Outbound: SMTP Proxy	40	24%	191
Outbound: Web Proxy	127	76%	606
Total	167	100%	797
Current DMDS Users	115	65%	

Table 4. User Survey Statistics

- Because of the high volume of messages, 24% of Naval messaging users will require an SMTP proxy at their command.
- 37.1% of DMS users access messaging from 1201Z-1400Z times (0700-0900 EST and 0200-0400 Hawaii Time). It appears that the majority of message readers access messaging from the East Coast first thing in the morning.

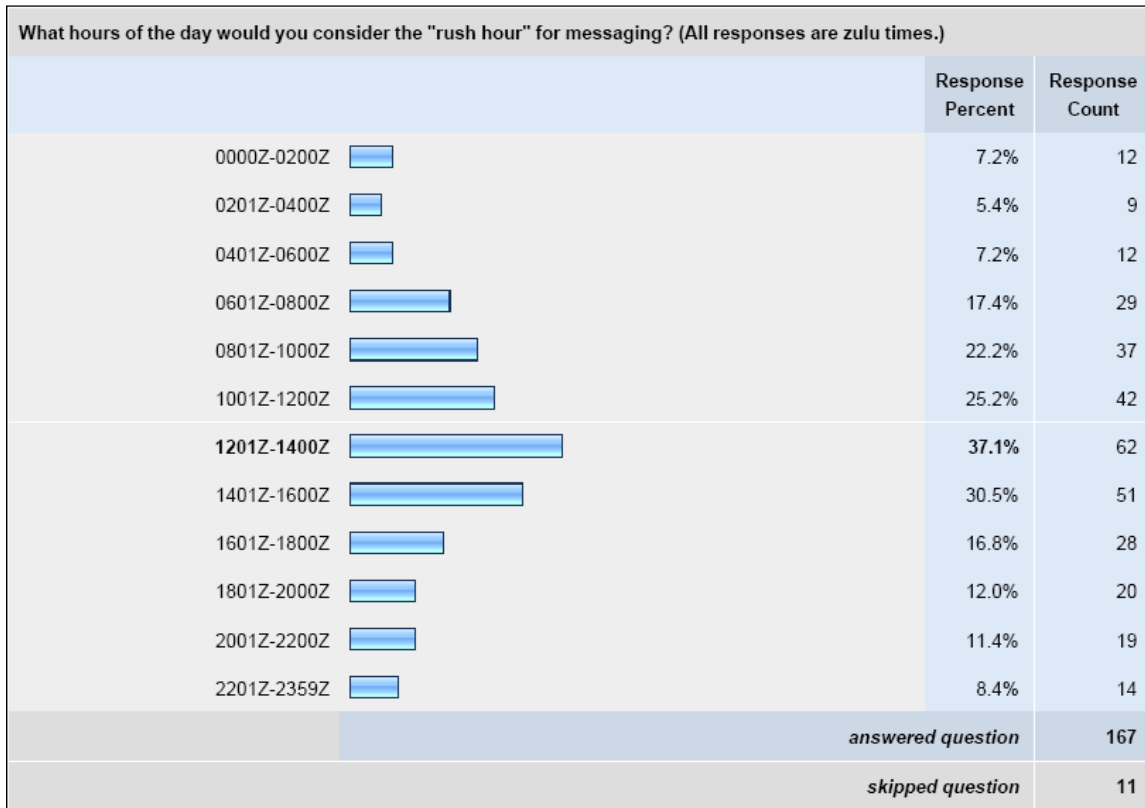


Figure 17. Naval Messaging Rush Hours

- 91.6% of respondents currently use DMS.
- The majority of message readers (67.1%) read their messages daily.

C. SUMMARY OF CONCLUSIONS

Chapter I presented our primary research objective: illustrate the functional contribution and change management process of the NREMS program implementation efforts in the Navy. To achieve this objective, this thesis posed two supporting research questions.

1. Architectural Transition Research

How does the Classic DMS to NREMS architecture change contribute to: (1) the CNO direction for consolidation of communications resources on home soil, and (2) the CNO direction to transition off of and close down legacy systems?

- What is the current Classic client server DMS architecture and where is it deployed?
- What is the current NREMS architecture, its technical advantages, and where will it be deployed?
- How does the NREMS implementation answer the CNO's direction and what are the key benefits in cost and performance?

The current DMS architecture set the stage for what the JCS now seeks in DOD communications, Net-centric Enterprise Services. The COTS based product development and the centralized services offered by DMS gave way to interoperable, cost effective, adaptable and flexible architecture that is no longer service unique. Although the DOD continues to seek further advantages in costs and maintainability, it is the shift from AUTODIN to DMS that affords the opportunity to extend the use of available and current technology to the end user while continuing to meet the DOD's operational requirements. NREMS allows the DOD to extend DMS's messaging capabilities without the onslaught of increased hardware installations, increased personnel support requirements, and significant cost overruns due to site specific requirements.

The existing technology allows the DOD to take advantage of proven reliable enterprise services that are currently in existence in the commercial industry. Although the system is presented with the shore based architecture in mind, the means to extend the network to at sea units or the Marine in the field is only constrained by the bandwidth available to the end user.

2. Business Process Transition Research

Evaluate the transition from DMS to NREMS.

- Is the transition plan from DMS to NREMS effective? What are its strengths and weaknesses?
- Determine Naval messaging organizations' business process. How can commands be differentiated to support appropriate levels of service in order to create the appropriate requirements document for contract awarded to support NREMS?

a. *The Transition Plan*

The transition plan was analyzed in Chapter III using Jick's change management framework.

The strengths of the transition plan include a detailed vision, a thorough implementation plan, a strong sense of urgency among the leadership, and an abundance of enabling structures to support the change effort. The detailed vision is a transition from a client-server architecture to a web-enabled messaging system that reduces infrastructural support requirements, centralizes resources and provides a uniform messaging system throughout the Navy. The NMWG has developed a simple, but detailed implementation plan with activities assigned and a time line for completion. The plan is flexible so that appropriate changes can be made as the transition progresses. The funding for legacy systems will be eliminated in fiscal year 2011. Therefore, it is imperative that Naval messaging transition to NREMS as quickly as possible. The NMWG and the Space and Naval Warfare Systems Command have information and training resources available for end user to access if desired. All of these factors will benefit the change process.

However, the transition plan has not addressed some areas of concern. A thorough understanding of the current Naval messaging enterprise (data about assets and

users) does not exist. The assets and resources procured in support of the transition are based on educated guesses. If inaccurate, transition efforts can suffer causing increased costs and implementation plan delays. No formal feedback system exists for change recipients to provide feedback. Transition plan information and resources are available in a pull format. This format is sufficient if change recipients buy-in to the proposed change. However, this is not the case. The fall out of the change efforts undertaken during the transition from AUTODIN to DMS is tremendous change recipient skepticism and resistance to change. This is not easily overcome. Current efforts are not sufficient to address a lack of change recipient buy-in.

b. Business Processes

In conjunction with the Space and Naval Warfare Systems Command, six businesses processes were defined as outlined in Chapter V. A Naval messaging user survey was conducted to gather data about the Naval messaging organization. This data was used to characterize the current Naval messaging process and determine the appropriate business process for an organization implementing NREMS. All user data and a user database were provided to Space and Naval Warfare Systems Command. The database can be maintained and edited to provide more current or additional information. Preformatted queries and reports were created in the database as well. As the database is updated, the queries can be rerun and reports generated to reflect the current status of Naval messaging.

3. Summary

In spite of some of the challenges with the architecture and change management plan, the transition

from DMS to NREMS has tremendous merit. The opportunities made available by the transition from AUTODIN to DMS (use of COTS products and proven technology) are consistent with DOD's transition to a Net-centric environment and Net-centric Enterprise Services. As evidence of successful implementations of NREMS progress throughout the Pacific theater, end users will institutionalize this significant step forward for Naval messaging.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. RECOMMENDATIONS

This chapter offers recommendations for further consideration.

A. FINDINGS

Architecturally there are technical issues that must be thoroughly reviewed and tested to ensure system is operating at peak performance level.

- CP-XP start time failures may become the Achilles hill for the system if the components are not tested for cause and effect.
- The ability of the system to handle failover while maintaining expected levels of performance could also cause high level damage if the AMHS's maximum capacity capabilities are discovered during a real wartime scenario when communications are vital.

These problems, however grave they may seem, can be tested, identified, and corrected or controlled with the proper implementation strategy. They only become high risks when the proper time and dollars are not directed to ensure the components performance quality attributes are met.

The core of the NREMS success will rest with high level support and implementation of supporting policies and procedures that will ensure the program succeeds. Pending infrastructure issues such as DOD PKI and NMCI connectivity are not based upon failed technical solutions. They are the direct result of bureaucratic policies and procedures that inhibit progress. The DMS transformation to NREMS is driven by increased cost savings, decreased maintenance requirements and improved personnel support issues. The program solves those issues and with the proper support can

meet and maybe even exceed DMS MROC 3-88 (technical), CJCSI 5721.01C (policy) and command user (operational) requirements.

Culturally, much remains to be done to convince change recipients that the NREMS project has merit. End users remain at best, apathetic, at worst skeptical and sometimes hostile, when introduced to the NREMS project. Although not a significant business process change, NREMS can still suffer from delayed implementation schedules if the change recipient does not cooperate fully and avail him/herself of the required training and resources available to ease the transition and assist in institutionalization of the new business process. The change culture of Naval messaging can create unanticipated expenditure of time and resources if not addressed properly, and an unwillingness to institutionalize the new business process. A thorough risk analysis of the potential impact of change recipient resistance would be appropriate to determine if current change efforts might be significantly impacted.

The database provided to the Space and Naval Warfare Systems Command offers the most current information available about the Naval messaging organization. As each Naval messaging command is visited during the transition, additional information can be added to the database and current information revised. This simple endeavor can easily address the lack of knowledge of the current Naval messaging organization.

B. RECOMMENDATIONS FOR FUTURE STUDY

- Past testing and evaluation of NREMS consisted of testing the AMHS core component only. The entire DMS architecture was tested in the JTIC lab. Recommend testing of the entire NREMS

architecture in the lab environment to determine that the NREMS product will meet critical quality attribute requirements.

- Evaluation of afloat activity bandwidth requirements for implementation of NREMS.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. SURVEY QUESTIONNAIRE

Defense Message System Organizational Data

[Exit this survey >>](#)

1. Informed Consent

Introduction. You are invited to participate in a study entitled Defense Message System Organizational Data by the Naval Postgraduate School in support of SPAWARSSYSCOM.

Procedures. In an effort to optimize resources and ensure that we can support you appropriately, the Navy Postgraduate School under guidance from PEO-PMW 160-3 has developed a survey to help us understand your command's business process for organization messaging. The results of this survey will be used to properly plan, route resources to where they are most needed, and identify an optimum business process for your command as the Navy transitions to a web-based messaging management system called Navy Regional Enterprise Messaging System (NREMS). This survey will take approximately 15 minutes to complete and is completely web-based.

Risks and Benefits. I understand that this project does not involve greater than minimal risk and involves no known reasonably foreseeable risks or hazards greater than those encountered in everyday life. I have also been informed of any benefits to myself or to others that may reasonably be expected as a result of this research.

Compensation. I understand that no tangible compensation will be given. I understand that a copy of the research results will be available at the conclusion of the experiment when requested of SPAWARSSYSCOM.

Confidentiality & Privacy Act. I understand that all records of this study will be kept confidential and that my privacy will be safeguarded. No personal information will be obtained or publicly accessible which could identify me as a participant. My responses will only be identified by PLA on all research forms/data bases. I understand that records of my participation will be maintained by NPS for three years, after which they will be destroyed.

Voluntary Nature of the Study. I understand that my participation is strictly voluntary, and if I agree to participate, I am free to withdraw at any time without prejudice.

Points of Contact. I understand that if I have any questions or comments regarding this project upon the completion of my participation, I should contact the Principal Investigator, LCDR Avonna S. Ramsey, asramsey@nps.edu. Any other questions or concerns may be addressed to the IRB Chair, LT Brent Olde, 656-3807, baolde@nps.edu.

Statement of Consent. I have been provided with a full explanation of the purpose, procedures, and duration of my participation in this research project. I understand how my identification will be safeguarded and have had all my questions answered. I have been provided a copy of this form for my records and I agree to participate in this study. I understand that by agreeing to participate in this research and signing this form, I do not waive any of my legal rights.

Click "Next" to get started with the survey. If you'd like to leave the survey at any time, just click "Exit this survey". Your answers will be saved.

* **1. Based on the information provided above, I consent to participate in this survey**

☐ I agree

Next >>

2. Types of users

The following questions are related to the number and type of users in your organization.

*** 2. Enter your organization's PLA.***** 3. How many message releasers does your organization have?**

- ☐ 0 - 5
- ☐ 6 - 10
- ☐ 11 - 20
- ☐ Greater than 20

4. Provide the total count of all message releasers for your PLA.*** 5. How many message drafters does you organization have?**

- ☐ 0 - 5
- ☐ 6 - 10
- ☐ 11 - 20
- ☐ Greater than 20

6. Provide the total count of all message drafters for your PLA.*** 7. How many message readers does your organization have?**

- ☐ 0 - 20
- ☐ 21 - 50
- ☐ 51 - 75
- ☐ Greater than 75

8. Provide the total count for all message readers for your PLA.

[<< Prev](#) [Next >>](#)

Defense Message System Organizational Data

[Exit this survey >>](#)

3. Messaging Activity

The following questions will help us determine your organization's requirements for accessing messages and searching the message archive.

* 9. What hours of the day would you consider the "rush hour" for messaging? (All responses are zulu times.)

- ☐ 0000Z-0200Z
- ☐ 0201Z-0400Z
- ☐ 0401Z-0600Z
- ☐ 0601Z-0800Z
- ☐ 0801Z-1000Z
- ☐ 1001Z-1200Z
- ☐ 1201Z-1400Z
- ☐ 1401Z-1600Z
- ☐ 1601Z-1800Z
- ☐ 1801Z-2000Z
- ☐ 2001Z-2200Z
- ☐ 2201Z-2359Z

10. Estimate the number of individuals in your organization that will read and search messages simultaneously, during the rush hour. Your response will help us to determine system load.

* 11. Do releasers, drafters and/or readers perform searches of messages?

- ☐ Yes
- ☐ No

12. Estimate the number of concurrent search queries that will be performed. (Readers performing searches simultaneously.)

[<< Prev](#) [Next >>](#)

Defense Message System Organizational Data

[Exit this survey >>](#)

4. Message Business Process

The following questions will assist us in characterizing the business process your organization uses for naval messaging.

* 13. Are messages delivered to a read board or public folder?

- ☐ Yes
☐ No

* 14. Are messages normally delivered to readers via email?

- ☐ Yes
☐ No

* 15. Do you currently use DMDS?

- ☐ Yes
☐ No

* 16. Do you currently receive messages via DMS?

- ☐ Yes
☐ No

* 17. How often does your average user check messages?

- ☐ Hourly
☐ Daily
☐ Weekly
☐ Monthly

[<< Prev](#) [Next >>](#)

5. Thanks!

I appreciate your feedback.

[<< Prev](#)

[Done >>](#)

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. SURVEY RESPONDENT DATA

PLA	Number of Message Releasers	Number of Message Drafters	Number of Message Readers	Read Board	Email	DMDS	DMS
63216	0 - 5	0 - 5	0 - 20	Yes	No	No	Yes
AEGIS TECHREP MOORESTOWN NJ	0 - 5	0 - 5	21 - 50	No	Yes	No	Yes
AEGIS TRAREDCEN DAHLGREN VA	0 - 5	11-20	Greater than 75	No	Yes	Yes	Yes
AIMD JACKSONVILLE FL	0 - 5	11-20	Greater than 75	Yes	No	No	Yes
AIMD KEY WEST(uc)	0 - 5	0 - 5	0 - 20	Yes	No	Yes	Yes
AIMD TRUAX CORPUS	6-10	0 - 5	Greater than 75	Yes	Yes	Yes	Yes
AIMD WHIDBEY ISLAND WA	0 - 5	11-20	Greater than 75	No	Yes	Yes	Yes
APL JHU LAUREL MD	Greater than 20	Greater than 20	Greater than 75	No	Yes	Yes	Yes
CENNAVAVNTECHTRA PENSACOLA FL	0 - 5	11-20	51 - 75	Yes	Yes	Yes	Yes
CENNAVLEADERSHIP DAM NECK VA	0 - 5	0 - 5	Greater than 75	Yes	No	Yes	Yes
CENSEABEESFACENG DET FT LEONARD WOOD MO	0 - 5	0 - 5	51 - 75	Yes	Yes	Yes	Yes
CENSURFDETPHILADEL PHIA, PA	0 - 5	0 - 5	0 - 20	No	No	No	Yes
CENTECTRAGRU DET ATSUGI	0 - 5	0 - 5	21 - 50	Yes	Yes	Yes	Yes
CMIONORFALKVA	0 - 5	11-20	0 - 20	Yes	Yes	Yes	Yes
CNATRA CORPUS CHRISTI TX	0 - 5	6-10	Greater than 75	Yes	No	Yes	Yes
CNATRA DET KINGSVILLE TX	0 - 5	0 - 5	0 - 20	No	Yes	Yes	Yes
CNATRADETCC	0 - 5	0 - 5	0 - 20	Yes	No	Yes	Yes
COM TWO TWO NCR	0 - 5	Greater than 20	51 - 75				
COMNAVAIRSYSCOM//6. 1.2.2	0 - 5	0 - 5	51 - 75	No	No	No	Yes
COMNAVAIRWARCENA CDIV PATUXENT RIVER MD	Greater than 20	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
COMNAVREG MIDLANT NORFOLK VA	11-20	Greater than 20	Greater than 75	Yes	Yes	No	No
COMNAVREG SW SAN DIEGO CA	Greater than 20	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
COMNAVSAFECEEN NORFOLK VA	0 - 5	0 - 5	Greater than 75	Yes	No	Yes	Yes
COMNAVSEASYSYSCOM WASHINGTON DC	6-10	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
COMNCWGRU TWO PORTSMOUTH VA	0 - 5	Greater than 20	Greater than 75	Yes	No	Yes	Yes
COMOMAG CORPUS CHRISTI TX	6-10	0 - 5	21 - 50	Yes	Yes	Yes	Yes
COMPACFLT PEARL HARBOR HI	Greater than 20	Greater than 20	Greater than 75	No	No	Yes	No
COMPATRECONWING ELEVEN	Greater than 20	Greater than 20	21 - 50	Yes	Yes	Yes	Yes
COMSPAWARSYSCOM SAN DIEGO CA	Greater than 20	Greater than 20	Greater than 75	No	Yes	Yes	Yes
COMSUBGRU EIGHT REP NORTHWOOD UK	0 - 5	6-10	0 - 20	No	Yes	Yes	Yes
COMTRAWING FIVE MILTON FL	0 - 5	11-20	Greater than 75	Yes	No	Yes	Yes

PLA	Number of Message Releasers	Number of Message Drafters	Number of Message Readers	Read Board	Email	DMDS	DMS
COMTRAWING TWO KINGSVILLE TX	0 - 5	0 - 5	21 - 50	Yes	Yes	Yes	Yes
DLD WC SUPP BREMERTON WA	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
DPTNAVSCI GLAKESMARICAD TRAVERSE CITY MI	0 - 5	0 - 5	0 - 20	No	No	No	Yes
EODMU SIX	0 - 5	11-20	Greater than 75				
EODMU SIX DET PANAMA CITY FL	0 - 5	0 - 5	0 - 20	Yes	No	Yes	Yes
FACSFAC VACAPES	6-10	Greater than 20	Greater than 75	Yes	No	Yes	Yes
FACSFAC VACAPES	11-20	11-20	21 - 50	Yes	Yes	Yes	Yes
FISC SIGONELLA IT	0 - 5	0 - 5	21 - 50	No	Yes	Yes	Yes
FLELOGSUPPRON FOUR SIX	0 - 5	11-20	21 - 50	No	Yes	Yes	Yes
HELSEACOMBATRON TWO	0 - 5	11-20	Greater than 75	Yes	No	Yes	Yes
HSL SIX ZERO MAYPORT FL	6-10	0 - 5	Greater than 75	Yes	Yes	No	Yes
MINWARTRACEN INGLESIDE TX (UC)	6-10	11-20	Greater than 75	No	Yes	No	Yes
MSCREP SEATTLE WA	0 - 5	0 - 5	0 - 20	Yes	No	Yes	Yes
MTCC CAMP LEJEUNE	Greater than 20	Greater than 20	51 - 75				
NACOPSPTCEN	0 - 5	6-10	21 - 50	Yes	No	Yes	Yes
NAS CORPUS CHRISTI TX	0 - 5	0 - 5	21 - 50	Yes	No	Yes	Yes
NAS JAX	11-20	Greater than 20	Greater than 75	Yes	No	Yes	Yes
NAS OCEANA VA	Greater than 20	Greater than 20	Greater than 75	Yes	No	Yes	No
NAVAMMOLOGCEN AMMOPAC SAN DIEGO CA	0 - 5	6-10	21 - 50	No	Yes	Yes	Yes
NAVAUDSVC WASHINGTON DC	0 - 5	Greater than 20	21 - 50	Yes	Yes	No	Yes
NAVBASE KITSAP SILVERDALE WA	Greater than 20	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
NAVCOMM DET CHINHAE KOR	0 - 5	6-10	0 - 20	No	Yes	Yes	Yes
NAVCOMTELSTA FAR EAST	0 - 5	Greater than 20	Greater than 75				
NAVCOMTELSTA FAR EAST	0 - 5	0 - 5	0 - 20	Yes	Yes	Yes	Yes
NAVCOMTELSTA FAR EAST YOKOSUKA JA	6-10	6-10	21 - 50				
NAVCOMTELSTA FAR EAST YOKOSUKA JA	0 - 5	6-10	21 - 50	Yes	Yes	Yes	Yes
NAVCOMTELSTA JACKSONVILLE DET KEY WEST FL	0 - 5	6-10	0 - 20	No	Yes	Yes	Yes
NAVCOMTELSTA NAPLES IT	11-20	6-10	Greater than 75	Yes	Yes	Yes	Yes
NAVCOMTELSTA SICILY IT	0 - 5	6-10	21 - 50	No	Yes	No	Yes
NAVCRUITDIST COLUMBUS OH	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NAVCRUITDIST DALLAS TX	0 - 5	0 - 5	0 - 20	No	Yes	Yes	Yes
NAVCRUITDIST NASH	0 - 5	0 - 5	21 - 50	No	Yes	Yes	Yes
NAVCRUITDIST SEATTLE WA	0 - 5	0 - 5	0 - 20	No	Yes	Yes	Yes
NAVCYBERDEFOPSCOM	11-20	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes

PLA	Number of Message Releasers	Number of Message Drafters	Number of Message Readers	Read Board	Email	DMDS	DMS
NORFOLK VA							
NAVDRUGLAB	0 - 5	0 - 5	0 - 20	No	No	No	Yes
NAVDRUGLAB GREAT LAKES IL	0 - 5	0 - 5	0 - 20	No	No	No	Yes
NAVDRUGLAB SAN DIEGO CA	11-20	11-20	0 - 20	No	No	No	Yes
NAVENVIRHLTHCEN PORTSMOUTH VA	0 - 5	6-10	21 - 50	Yes	Yes	Yes	No
NAVFLIGHTDEMRON	0 - 5	6-10	21 - 50	Yes	Yes	Yes	Yes
NAVHOSP LEMOORE CA	0 - 5	11-20	Greater than 75	No	Yes	No	Yes
NAVLEGSVCOFF MIDLANT NORFOLK VA	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NAVLEGSVCOFF SE JACKSONVILLE FL	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NAVMARCORESCEN LEHIGH VALLEY PA	0 - 5	6-10	Greater than 75	Yes	Yes	Yes	Yes
NAVMEDIACENFSD NORFOLK VA	0 - 5	0 - 5	0 - 20	No	No	No	Yes
NAVMEDIACENSANDIE GO(UC)	0 - 5	0 - 5	0 - 20	Yes	No	No	Yes
NAVNUPWRTACOM	6-10	6-10	Greater than 75	Yes	No	No	Yes
NAVOPMEDINST DET SURFWARMEDINST	0 - 5	0 - 5	0 - 20	No	Yes	No	No
NAVOPSCENPIT	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NAVOPSPTCEN DETROIT MI	0 - 5	0 - 5	21 - 50	No	Yes	Yes	Yes
NAVOPSPTCEN GULFPORT MS	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NAVOPSPTCEN PEORIA IL	0 - 5	6-10	0 - 20	No	Yes	Yes	Yes
NAVOPSPTCEN WHIDBEY ISLAND WA	0 - 5	0 - 5	0 - 20	Yes	Yes	Yes	Yes
NAVOPSPTCENERIE	0 - 5	0 - 5	0 - 20	No	No	Yes	Yes
NAVOPSPTCENFND	0 - 5	0 - 5	Greater than 75	Yes	Yes	Yes	Yes
NAVOPHTALSUPPTRAC T YORKTOWN VA	0 - 5	6-10	Greater than 75	Yes	Yes	Yes	Yes
NAVOSP CHERRY PT NC	0 - 5	0 - 5	0 - 20	Yes	Yes	No	Yes
NAVPERSEVCOM NORFOLK VA	0 - 5	Greater than 20	21 - 50	Yes	Yes	Yes	Yes
NAVPTO PENSACOLA FL	0 - 5	0 - 5	0 - 20	No	No	No	Yes
NAVRESREDCOM MIDLANT WASHINGTON DC	11-20	11-20	21 - 50	Yes	Yes	No	Yes
NAVSATCOMMFAC NORTHWEST VA	0 - 5	0 - 5	21 - 50	Yes	Yes	Yes	Yes
NAVSEA DET RASO YORKTOWN VA	0 - 5	0 - 5	0 - 20	Yes	No	No	Yes
NAVSEA INACTSHIPMAINTO PEARL HARBOR HI	0 - 5	0 - 5	0 - 20	Yes	Yes	No	Yes
NAVSEA INACTSHIPMAINTO PHILADELPHIA PA	0 - 5	0 - 5	0 - 20	Yes	No	No	Yes
NAVSEA INACTSHIPOFF PORTSMOUTH VA	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NAVSEA INACTSHIPOFF PORTSMOUTH VA	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NAVSPECWARCEN DET SDV PANAMA CITY FL.	0 - 5	0 - 5	21 - 50	Yes	Yes	Yes	Yes
NAVSTA INGLESIDE TX	0 - 5	Greater than 20	Greater than 75	No	Yes	Yes	Yes

PLA	Number of Message Releasers	Number of Message Drafters	Number of Message Readers	Read Board	Email	DMDS	DMS
NAVSTA NORFOLK VA	Greater than 20	Greater than 20	Greater than 75	Yes	No	Yes	Yes
NAVSUBSUPPFAC NEW LONDON CT	0 - 5	0 - 5	51 - 75	No	Yes	Yes	No
NAVSUPPACT PERSUPPDET NEW ORLEANS LA	0 - 5	0 - 5	0 - 20	Yes	Yes	Yes	Yes
NAVSURFWARCEN DET BREMERTON	0 - 5	0 - 5	21 - 50	Yes	Yes	Yes	Yes
NAVSURFWARCEN PHDIV VIRGINIA BEACH VA	0 - 5	11-20	21 - 50	No	No	No	Yes
NAVSURFWARCEN PORT HUENEME DIV DET LOUISVILLE KY	0 - 5	6-10	Greater than 75	No	Yes	Yes	Yes
NAVSURFWARCEN SHIPSYSNGSTA PHILADELPHIA PA	0 - 5	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
NAVSURFWARCENDIV INDIAN HEAD	0 - 5	0 - 5	21 - 50				
NAVTREATYSUPPORT INDIAN HEAD MD	0 - 5	6-10	0 - 20	No	No	Yes	Yes
NAVUNSEAWARCEN DET AUTEC ANDROS ISLAND BAHAMAS	11-20	11-20	51 - 75				
NAVUNSEAWARCENDIV KEYPORT WA	Greater than 20	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
NAVY BAND WASHINGTON DC	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NAVY GSM	6-10	6-10	0 - 20	Yes	Yes	Yes	Yes
NCTAMS LANT DET SOUDA BAY GR	0 - 5	0 - 5	0 - 20	No	Yes	Yes	Yes
NCTAMS LANT Norfolk VA	Greater than 20	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
NCTAMS LANT NORFOLK VA	Greater than 20	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
NCTAMS LANT NORFOLK VA	Greater than 20	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
NCTAMSLANTDETGTMO	0 - 5	0 - 5	21 - 50	Yes	Yes	Yes	Yes
NCTAMSPAC	Greater than 20	Greater than 20	Greater than 75				
NETPDTC	0 - 5	Greater than 20	Greater than 75	Yes	No	Yes	Yes
NETSAFA PENSACOLA FL	0 - 5	11-20	21 - 50	No	Yes	Yes	Yes
NETWARCOM NORFOLK VA	Greater than 20	Greater than 20	Greater than 75				
NMCB 18	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NMCCEDSP	0 - 5	0 - 5	21 - 50	No	Yes	Yes	Yes
NMSC DET MILMEDSUPPOFF GREAT LAKES IL	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NOSC ERIE	0 - 5	0 - 5	0 - 20	Yes	No	Yes	Yes
NOSC PEORIA	6-10	6-10	0 - 20	No	Yes	Yes	Yes
NOSC WILMINGTON DE	0 - 5	0 - 5	0 - 20	Yes	No	Yes	Yes
NRL DET STENNIS SPACE CENTER MS	0 - 5	0 - 5	21 - 50	No	Yes	No	Yes
NRL WASHINGTON DC	11-20	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
NROTC NORTH CAROLINA PIEDMONT REGION	0 - 5	0 - 5	21 - 50	Yes	Yes	Yes	Yes
NROTC NOTRE DAME UNIVERSITY	0 - 5	0 - 5	0 - 20	No	Yes	Yes	Yes

PLA	Number of Message Releasers	Number of Message Drafters	Number of Message Readers	Read Board	Email	DMDS	DMS
NROTCU CARNEGIE MELLON UNIV PITTSBURGH PA	0 - 5	6-10	0 - 20	Yes	No	No	Yes
NROTCU CHICAGO AREA EVANSTON IL	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NROTCU HOLY CROSS WORCESTER MA	0 - 5	0 - 5	0 - 20	Yes	Yes	Yes	Yes
NROTCU IOWA STATE UNIV AMES IA	0 - 5	0 - 5	0 - 20	No	No	No	Yes
NROTCU JACKSONVILLE UNIV JACKSONVILLE FL	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NROTCU LOS ANGELES CA	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NROTCU MARQUETTE UNIV	0 - 5	0 - 5	0 - 20	Yes	Yes	Yes	Yes
NROTCU NORTH CAROLINA PIEDMONT REGION DURHAM NC	0 - 5	0 - 5	0 - 20	Yes	Yes	No	Yes
NROTCU PURDUE UNIV WEST LAFAYETTE IN	0 - 5	0 - 5	0 - 20	No	Yes	Yes	Yes
NROTCU PURDUE UNIV WEST LAFAYETTE IN	6-10	6-10	0 - 20	Yes	Yes	No	Yes
NROTCU SOUTHERN UNIV BATON ROUGE LA	0 - 5	0 - 5	0 - 20	No	Yes	No	No
NROTCU UNIV OF MICHIGAN	0 - 5	0 - 5	0 - 20	Yes	Yes	Yes	No
NROTCU UNIV OF NEBRASKA LINCOLN NE	0 - 5	0 - 5	0 - 20	No	Yes	No	Yes
NROTCU UNIVERSITY OF MINNESOTA	0 - 5	0 - 5	0 - 20	No	No	No	Yes
NROTCU VMI	0 - 5	0 - 5	0 - 20	No	No	Yes	Yes
NSSC NORFOLK VA	11-20	Greater than 20	Greater than 75	No	Yes	Yes	No
OTC NEWPORT	0 - 5	Greater than 20	Greater than 75	No	Yes	Yes	Yes
PATRON NINE	6-10	Greater than 20	Greater than 75	Yes	No	No	Yes
PATRON THREE ZERO	0 - 5	11-20	Greater than 75	Yes	Yes	Yes	Yes
PERSUPP DET BRUNSWICK ME	11-20	Greater than 20	21 - 50	Yes	Yes	Yes	Yes
PERSUPP DET CORPUS CHRISTI TX	0 - 5	0 - 5	21 - 50	Yes	Yes	Yes	Yes
PERSUPP DET FT GEORGE G MEADE MD	0 - 5	11-20	21 - 50	No	Yes	Yes	Yes
PERSUPP DET INGLESIDE TX	0 - 5	6-10	0 - 20	No	Yes	Yes	Yes
PERSUPP DET NEWPORT RI	6-10	0 - 5	0 - 20	No	Yes	Yes	Yes
PERSUPPDET KEY WEST	0 - 5	11-20	0 - 20	No	Yes	Yes	Yes
PERSUPPDET PATUXENT RIVER MD	0 - 5	11-20	21 - 50	Yes	Yes	Yes	No
PHIBCB-2	0 - 5	0 - 5	21 - 50	Yes	No	Yes	Yes
RESOPTCENMIAMI 61927	0 - 5	0 - 5	0 - 20	No	Yes	Yes	Yes
RLSO MID-ATLANTIC NORFOLK VA	0 - 5	6-10	Greater than 75	No	Yes	Yes	Yes
SEACONWEPSCOL JACKSONVILLE FL	0 - 5	0 - 5	21 - 50	Yes	No	Yes	Yes
SOUTHEAST RMC MAYPORT FL	Greater than 20	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
SOUTHWEST RMC SAN DIEGO	Greater than 20	Greater than 20	21 - 50	Yes	No	Yes	Yes
SPAWARSYSCEN CHARLESTON SC	Greater than 20	Greater than 20	Greater than 75	No	Yes	Yes	Yes
SPAWARSYSCEN	6-10	6-10	0 - 20	No	No	No	No

PLA	Number of Message Releasers	Number of Message Drafters	Number of Message Readers	Read Board	Email	DMDS	DMS
CHASN, Code 523							
SPAWARSSYSCEN SAN DIEGO CA	Greater than 20	Greater than 20	Greater than 75	No	Yes	Yes	Yes
SPEC PROJ PATRON ONE	11-20	11-20	Greater than 75				
STRKFITRON ONE FIVE FOUR	11-20	Greater than 20	Greater than 75	Yes	No	Yes	Yes
SUBTORPFACYORKTOW N VA	0 - 5	0 - 5	21 - 50	Yes	Yes	Yes	No
SUPPLY SUPBN TWO WEST HARTFORD CT	0 - 5	0 - 5	0 - 20	Yes	No	No	Yes
TRANSITPERSU GLAKES	0 - 5	6-10	21 - 50	No	Yes	Yes	Yes
TRARON TWO TWO	0 - 5	Greater than 20	51 - 75				
TRARONFOUR PENSACOLA FL	0 - 5	0 - 5	21 - 50	No	Yes	Yes	Yes
TRIREFAC KINGS BAY	11-20	Greater than 20	Greater than 75	No	Yes	Yes	Yes
TRITRAFAC BANGOR WA/TSD PACNORWEST BANGOR WA	11-20	Greater than 20	0 - 20	Yes	No	No	No
USNA ANNAPOLIS MD	Greater than 20	Greater than 20	51 - 75	No	Yes	Yes	Yes
USS BLUE RIDGE / COMSEVENTHFLT	Greater than 20	Greater than 20	Greater than 75	Yes	Yes	Yes	No
We guard for over 100 PLA's	Greater than 20	Greater than 20	Greater than 75	Yes	Yes	Yes	Yes
WPNSTA CHARLESTON NC	Greater than 20	Greater than 20	Greater than 75	No	Yes	Yes	Yes

APPENDIX C. SURVEYMONKEY.COM SUMMARY REPORT

Defense Message System Organizational Data

Defense Message System Organizational Data

Based on the information provided above, I consent to participate in this survey		
	Response Percent	Response Count
I agree 	100.0%	178
answered question		178
skipped question		0

Enter your organization's PLA.		
		Response Count
		178
	answered question	178
	skipped question	0

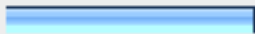
How many message releasers does your organization have?		
	Response Percent	Response Count
0 - 5 	70.2%	125
6 - 10 	7.9%	14
11 - 20 	8.4%	15
Greater than 20 	13.5%	24
answered question		178
skipped question		0

Provide the total count of all message releasers for your PLA.		
		Response Count
		170
	answered question	170
	skipped question	8

Defense Message System Organizational Data

How many message drafters does your organization have?		
	Response Percent	Response Count
0 - 5 	47.2%	84
6 - 10 	14.6%	26
11 - 20 	12.4%	22
Greater than 20 	25.8%	46
answered question		178
skipped question		0

Provide the total count of all message drafters for your PLA.		Response Count
		170
answered question		170
skipped question		8

How many message readers does your organization have?		
	Response Percent	Response Count
0 - 20 	39.3%	70
21 - 50 	23.0%	41
51 - 75 	5.1%	9
Greater than 75 	32.6%	58
answered question		178
skipped question		0

Provide the total count for all message readers for your PLA.		Response Count
		167
answered question		167
skipped question		11

Defense Message System Organizational Data

What hours of the day would you consider the "rush hour" for messaging? (All responses are zulu times.)			Response Percent	Response Count
0000Z-0200Z			7.2%	12
0201Z-0400Z			5.4%	9
0401Z-0600Z			7.2%	12
0601Z-0800Z			17.4%	29
0801Z-1000Z			22.2%	37
1001Z-1200Z			25.2%	42
1201Z-1400Z			37.1%	62
1401Z-1600Z			30.5%	51
1601Z-1800Z			16.8%	28
1801Z-2000Z			12.0%	20
2001Z-2200Z			11.4%	19
2201Z-2359Z			8.4%	14
answered question				167
skipped question				11

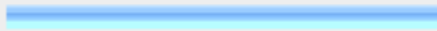
Estimate the number of individuals in your organization that will read and search messages simultaneously, during the rush hour. Your response will help us to determine system load.		Response Count
		157
answered question		157
skipped question		21

Defense Message System Organizational Data

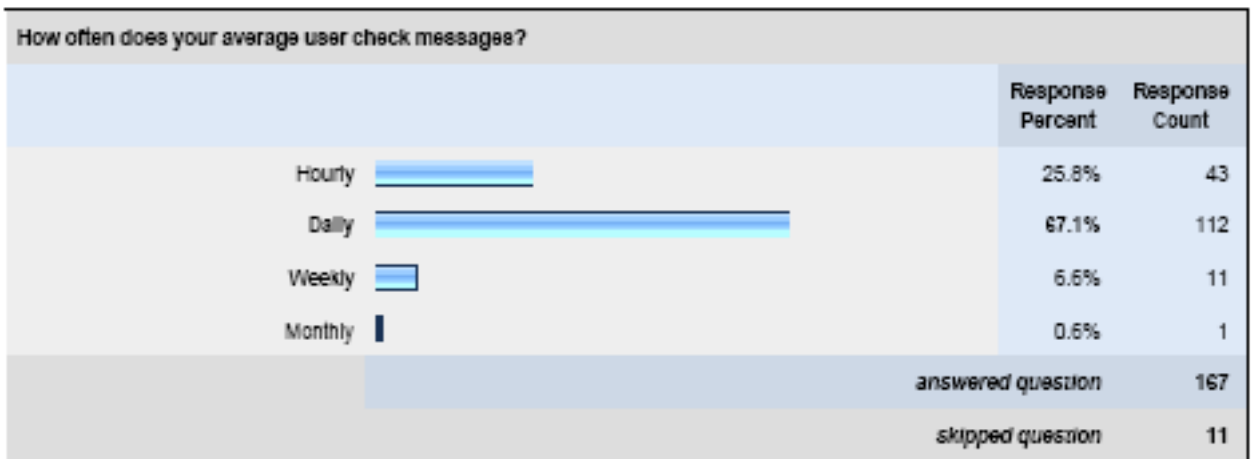
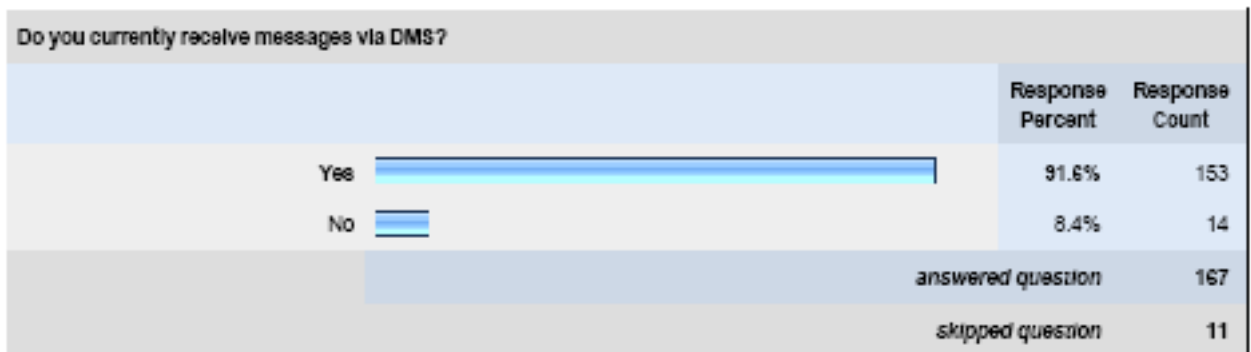
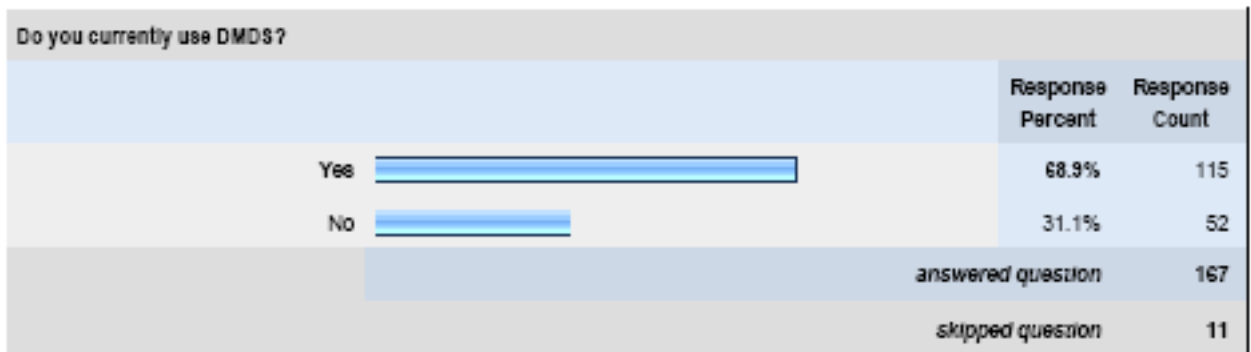
Do releasers, drafters and/or readers perform searches of messages?		
	Response Percent	Response Count
Yes 	68.3%	114
No 	31.7%	53
	answered question	167
	skipped question	11

Estimate the number of concurrent search queries that will be performed. (Readers performing searches simultaneously.)		
		Response Count
		150
	answered question	150
	skipped question	28

Are messages delivered to a read board or public folder?		
	Response Percent	Response Count
Yes 	53.3%	89
No 	46.7%	78
	answered question	167
	skipped question	11

Are messages normally delivered to readers via email?		
	Response Percent	Response Count
Yes 	70.7%	118
No 	29.3%	49
	answered question	167
	skipped question	11

Defense Message System Organizational Data



THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. SQL QUERIES DEVELOPED IN MICROSOFT ACCESS

The following are the SQL queries developed used the query design wizard to determine the business process type for each respondent:

- Outbound: SMTP Proxy
Inbound: DMDS Folder Delivery
(< 20 Releasers)

```
SELECT SurveyResults.ResultsID, SurveyResults.PLA,  
SurveyResults.NumberofMessageReleasers, SurveyResults.NumberofMessageDrafters,  
SurveyResults.NumberofMessageReaders, SurveyResults.ReadBoard,  
SurveyResults.Email, SurveyResults.DMDS, SurveyResults.DMS  
FROM SurveyResults  
WHERE ((Not (SurveyResults.NumberofMessageReleasers)="greater than 20") AND  
((SurveyResults.NumberofMessageDrafters)="Greater than 20") AND  
((SurveyResults.ReadBoard)="yes"));
```

- Outbound: SMTP Proxy
Inbound: DMDS Folder Delivery
(> 20 Releasers)

```
SELECT SurveyResults.ResultsID, SurveyResults.PLA,  
SurveyResults.NumberofMessageReleasers, SurveyResults.NumberofMessageDrafters,  
SurveyResults.NumberofMessageReaders, SurveyResults.ReadBoard,  
SurveyResults.Email, SurveyResults.DMDS, SurveyResults.DMS  
FROM SurveyResults  
WHERE (((SurveyResults.NumberofMessageReleasers)="greater than 20") AND  
((SurveyResults.ReadBoard)="yes"));
```

- Outbound: SMTP Proxy
Inbound: DMDS User Delivery
(< 20 Releasers)

```
SELECT SurveyResults.*, SurveyResults.ResultsID, SurveyResults.PLA,  
SurveyResults.NumberofMessageReleasers, SurveyResults.NumberofMessageDrafters,  
SurveyResults.NumberofMessageReaders, SurveyResults.ReadBoard,  
SurveyResults.Email, SurveyResults.DMDS, SurveyResults.DMS
```

```
FROM SurveyResults
```

```
WHERE ((Not (SurveyResults.NumberofMessageReleasers)="greater than 20") AND  
((SurveyResults.NumberofMessageDrafters)="greater than 20") AND  
((SurveyResults.ReadBoard)="no"));
```

- Outbound: SMTP Proxy
Inbound: DMDS User Delivery
(> 20 Releasers)

```
SELECT SurveyResults.*, SurveyResults.ResultsID, SurveyResults.PLA,  
SurveyResults.NumberofMessageReleasers, SurveyResults.NumberofMessageDrafters,  
SurveyResults.NumberofMessageReaders, SurveyResults.ReadBoard,  
SurveyResults.Email, SurveyResults.DMDS, SurveyResults.DMS
```

```
FROM SurveyResults
```

```
WHERE (((SurveyResults.NumberofMessageReleasers)="greater than 20") AND  
((SurveyResults.ReadBoard)="no"));
```

- Outbound: Web Proxy
Inbound: DMDS Folder Delivery

```
SELECT SurveyResults.*, SurveyResults.ResultsID, SurveyResults.PLA,  
SurveyResults.NumberofMessageReleasers, SurveyResults.NumberofMessageDrafters,  
SurveyResults.NumberofMessageReaders, SurveyResults.ReadBoard,  
SurveyResults.Email, SurveyResults.DMDS, SurveyResults.DMS
```

```
FROM SurveyResults
```

```
WHERE ((Not (SurveyResults.NumberofMessageReleasers)="greater than 20") AND  
(Not (SurveyResults.NumberofMessageDrafters)="greater than 20") AND (Not  
(SurveyResults.NumberofMessageReaders)="0 - 20") AND  
((SurveyResults.ReadBoard)="YES"));
```

- Outbound: Web Proxy
Inbound: DMDS User Delivery

```

SELECT SurveyResults.*, SurveyResults.ResultsID, SurveyResults.PLA,
SurveyResults.NumberofMessageReleasers,
SurveyResults.NumberofMessageDrafters,
SurveyResults.NumberofMessageReaders, SurveyResults.ReadBoard,
SurveyResults.Email, SurveyResults.DMDS, SurveyResults.DMS
FROM SurveyResults
WHERE (((SurveyResults.NumberofMessageReleasers)<>"greater than 20")
AND ((SurveyResults.NumberofMessageDrafters)<>"greater than 20") AND
((SurveyResults.NumberofMessageReaders)<>"0 - 20") AND
((SurveyResults.ReadBoard)="no"));

```

- Outbound: Web Proxy
Inbound: Web Bulletin Board Delivery

```

SELECT SurveyResults.*, SurveyResults.ResultsID, SurveyResults.PLA,
SurveyResults.NumberofMessageReleasers,
SurveyResults.NumberofMessageDrafters,
SurveyResults.NumberofMessageReaders, SurveyResults.ReadBoard,
SurveyResults.Email, SurveyResults.DMDS, SurveyResults.DMS
FROM SurveyResults
WHERE (((SurveyResults.NumberofMessageReleasers)<>"greater than 20")
AND ((SurveyResults.NumberofMessageDrafters)<>"greater than 20") AND
((SurveyResults.NumberofMessageReaders)="0 - 20") AND
((SurveyResults.ReadBoard)="yes"));

```

- Outbound: Web Proxy
Inbound: Web User Delivery

```

SELECT SurveyResults.*, SurveyResults.ResultsID, SurveyResults.PLA,
SurveyResults.NumberofMessageReleasers,
SurveyResults.NumberofMessageDrafters,
SurveyResults.NumberofMessageReaders, SurveyResults.ReadBoard,
SurveyResults.Email, SurveyResults.DMDS, SurveyResults.DMS
FROM SurveyResults
WHERE (((SurveyResults.NumberofMessageReleasers)<>"greater than 20")
AND ((SurveyResults.NumberofMessageDrafters)<>"greater than 20") AND
((SurveyResults.NumberofMessageReaders)="0 - 20") AND
((SurveyResults.ReadBoard)="no"));

```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. REPORTS GENERATED IN MICROSOFT ACCESS
FOR EACH BUSINESS PROCESS

***Outbound: SMTP Proxy
Inbound: DMDS User Delivery
(< 20 Releasers)***

PLA

NAVSTA INGLESIDE TX
NSSC NORFOLK VA
OTC NEWPORT
TRIREFFAC KINGS BAY

Count: ***4***

***Outbound: SMTP Proxy
Inbound: DMDS User Delivery
(> 20 Releasers)***

PLA

APL JHU LAUREL MD
COMPACFLT PEARL HARBOR HI
COMSPAWARSSCOM SAN DIEGO CA
SPAWARSSCEN CHARLESTON SC
SPAWARSSCEN SAN DIEGO CA
USNA ANNAPOLIS MD
WPNSTA CHARLESTON NC

Count: ***7***

Outbound: SMTP Proxy Inbound: DMDS Folder Delivery (> 20 Releasers)

PLA

COMNAVAIRWARCENACDIV PATUXENT RIVER MD

COMNAVREG SW SAN DIEGO CA

COMPATRECONWING ELEVEN

NAS OCEANA VA

NAVBASE KITSAP SILVERDALE WA

NAVSTA NORFOLK VA

NAVUNSEAWARCENDIV KEYPORT WA

NCTAMS LANT Norfolk VA

NCTAMS LANT NORFOLK VA

NCTAMS LANT NORFOLK VA

SOUTHEAST RMC MAYPORT FL

SOUTHWEST RMC SAN DIEGO

USS BLUE RIDGE / COMSEVENTHFLT

We guard for over 100 PLA's

Count: 14

***Outbound: SMTP Proxy
Inbound: DMDS Folder Delivery
(< 20 Releasers)***

PLA

COMNAVREG MIDLANT NORFOLK VA

COMNAVSEASYS COM WASHINGTON DC

COMNCWGRU TWO PORTSMOUTH VA

FACSFAC VACAPES

NAS JAX

NAVAUDSVC WASHINGTON DC

NAVCYBERDEFOPSCOM NORFOLK VA

NAVPERSDEVCOM NORFOLK VA

NAVSURFWARCEN SHIPSYSENGSTA PHILADELPHIA PA

NETPDTC

NRL WASHINGTON DC

PATRON NINE

PERSUPP DET BRUNSWICK ME

STRKFITRON ONE FIVE FOUR

TRITRAFAC BANGOR WATSD PACNORWEST BANGOR WA

Count: 15

Outbound: Web Proxy

Inbound: DMDS Folder Delivery

PLA

AIMD JACKSONVILLE FL

AIMD TRUAX CORPUS

CENNAVAVNTECHTRA PENSACOLA FL

CENNAVLEADERSHIP DAM NECK VA

CENSEABEESFACENG DET FT LEONARD WOOD MO

CENTECTRAGRU DET ATSUGI

CNATRA CORPUS CHRISTI TX

COMNAVSAFECEN NORFOLK VA

COMOMAG CORPUS CHRISTI TX

COMTRAWING FIVE MILTON FL

COMTRAWING TWO KINGSVILLE TX

FACSFAC VACAPES

HELSEACOMBATRON TWO

HSL SIX ZERO MAYPORT FL

NACOPSPTCEN

NAS CORPUS CHRISTI TX

NAVCOMTELSTA FAR EAST YOKOSUKA JA

NAVCOMTELSTA NAPLES IT

NAVENVIRHLTHCEN PORTSMOUTH VA

NAVFLIGHTDEMIRON

NAVMARCORESCEN LEHIGH VALLEY PA

NAVNUPWRTACOM

NAVOPSPTCENFND

NAVOPHTHALSUPTRACT YORKTOWN VA

NAVRESREDCOM MIDLANT WASHINGTON DC

NAVSATCOMMFAC NORTHWEST VA
NAVSPECWARCEN DET SDV PANAMA CITY FL.
NAVSURFWARCEN DET BREMERTON
NCTAMSLANTDETGTMO
NROTC NORTH CAROLINA PIEDMONT REGION
PATRON THREE ZERO
PERSUPP DET CORPUS CHRISTI TX
PERSUPPDET PATUXENT RIVER MD
PHIBCB-2
SEACONWEPSCOL JACKSONVILLE FL
SUBTORPFACYORKTOWN VA

Count: 36

Outbound: Web Proxy

Inbound: DMDS User Delivery

PLA

AEGIS TECHREP MOORESTOWN NJ
AEGIS TRAREDCEN DAHLGREN VA
AIMD WHIDBEY ISLAND WA
COMNAVAIRSYSCOM//6.1.2.2
FISC SIGONELLA IT
FLELOGSUPPRON FOUR SIX
MINWARTRACEN INGLESIDE TX (UC)
NAVAMMOLOGCEN AMMOPAC SAN DIEGO CA
NAVCOMTELSTA SICILY IT
NAVCRUITDIST NASH
NAVHOSP LEMOORE CA
NAVOPSPTCEN DETROIT MI
NAVSUBSUPPFAC NEW LONDON CT
NAVSURFWARCEN PHDIV VIRGINIA BEACH VA
NAVSURFWARCEN PORT HUENEME DIV DET LOUISVILLE KY
NETSAFA PENSACOLA FL
NMCCEDSP
NRL DET STENNIS SPACE CENTER MS
PERSUPP DET FT GEORGE G MEADE MD
RLSO MID-ATLANTIC NORFOLK VA
TRANSITPERSU GLAKES
TRARONFOUR PENSACOLA FL

Count: ***22***

Outbound: Web Proxy

Inbound: Web Bulletin Board Delivery

PLA

63216

AIMD KEY WEST(uc)

CMIONORFALKVA

CNATRADETCC

EODMU SIX DET PANAMA CITY FL

MSCREP SEATTLE WA

nAVCOMTELSTA FAR EAST

NAVMEDIACENSANDIEGO(UC)

NAVOPSPTCEN WHIDBEY ISLAND WA

NAVOSP CHERRY PT NC

NAVSEA DET RASO YORKTOWN VA

NAVSEA INACTSHIPMAINTO PEARL HARBOR HI

NAVSEA INACTSHIPMAINTO PHILADELPHIA PA

NAVSUPPACT PERSUPPDET NEW ORLEANS LA

NAVY GSM

NOSC ERIE

NOSC WILMINGTON DE

NROTCU CARNEGIE MELLON UNIV PITTSBURGH PA

NROTCU HOLY CROSS WORCESTER MA

NROTCU MARQUETTE UNIV

NROTCU NORTH CAROLINA PIEDMONT REGION DURHAM NC

NROTCU PURDUE UNIV WEST LAFAYETTE IN

NROTCU UNIV OF MICHIGAN

SUPPLY SUPBN TWO WEST HARTFORD CT

Count: 24

Outbound: Web Proxy

Inbound: Web User Delivery

PLA

CENSURFDETPHILADELPHIA, PA
CNATRA DET KINGSVILLE TX
COMSUBGRU EIGHT REP NORTHWOOD UK
DLD WC SUPP BREMERTON WA
DPTNAVSCI GLAKESMARICAD TRAVERSE CITY MI
NAVCOMM DET CHINHAE KOR
NAVCOMTELSTA JACKSONVILLE DET KEY WEST FL
NAVCUITDIST COLUMBUS OH
NAVCUITDIST DALLAS TX
NAVCUITDIST SEATTLE WA
NAVDRUGLAB
NAVDRUGLAB GREAT LAKES IL
NAVDRUGLAB SAN DIEGO CA
NAVLEGSVCOFF MIDLANT NORFOLK VA
NAVLEGSVCOFF SE JACKSONVILLE FL
NAVMEDIACENFSD NORFOLK VA
NAVOPMEDINST DET SURFWARMEDINST
NAVOPSCENPIT
NAVOPSPTCEN GULFPORT MS
NAVOPSPTCEN PEORIA IL
NAVOPSPTCENERIE
NAVPTO PENSACOLA FL
NAVSEA INACTSHIPOFF PORTSMOUTH VA
NAVSEA INACTSHIPOFF PORTSMOUTH VA
NAVTEATYSUPPORT INDIAN HEAD MD
NAVY BAND WASHINGTON DC
NCTAMS LANT DET SOUDA BAY GR
NMCB 18
NMSC DET MILMEDSUPPOFF GREAT LAKES IL
NOSC PEORIA
NROTC NOTRE DAME UNIVERSITY
NROTCU CHICAGO AREA EVANSTON IL
NROTCU IOWA STATE UNIV AMES IA
NROTCU JACKSONVILLE UNIV JACKSONVILLE FL
NROTCU LOS ANGELES CA

NROTCU PURDUE UNIV WEST LAFAYETTE IN
NROTCU SOUTHERN UNIV BATON ROUGE LA
NROTCU UNIV OF NEBRASKA LINCOLN NE
NROTCU UNIVERSITY OF MINNESOTA
NROTCU VMI
PERSUPP DET INGLESIDE TX
PERSUPP DET NEWPORT RI
PERSUPPDET KEY WEST
RESOPTCENMIAMI 61927
SPAWARSYSCEN CHASN, Code 523

Count: 45

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

(CJCSI) U.S. Department of Defense. Chairman of Joint Chiefs of Staff Instruction (CJCSI) 5721.01C. 2005. *Defense Message System and Associated Legacy Message Processing Systems*. (2005) Washington, D.C.

(Commander, Naval Network and Space Operations Command (CNNSOC). NTP 22A) Naval Telecommunications Publication (NTP) 22(A). (2003). *Defense Message System Local Operations and Network Management Policies and Procedures NTP 22(A)*. Produced by the Washington, D.C. Commander, Naval Network and Space Operations Command (CNNSOC).

(OCD) Automated Message Handling System (AMHS) Operational Concept Document (OCD) and Architectural Outline. (2004)

(TAIS) Defense Message System Architecture Working Group (DMSAWG). 1990. *The Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS)*. (1998) Washington, D.C.

"Defense Message System (DMS) FY97 Annual Report." Director, Operational Test and Evaluation (DOT&E). Defense Message System (DMS), FY97 Annual Report. (1997). Available at <http://www.globalsecurity.org/military/library/budget/fy1997/dot-e/other/97dms.html>; Internet; accessed 10 October 2006.

"Defense Message System (DMS)." Defense Information System Agency (DISA). Available at <http://www.disa.mil/main/prodsol/dms.html>; Internet; accessed 23 October 2006.

Bass, L., Nord, R., Wood, W., and Zubrow, D. 2006. *Risk Themes Discovered Through Architecture Evaluations*. Carnegie Mellon Software Engineering Institute Technical Report. Available at: <http://www.sei.cmu.edu/publications/documents/06.reports/06tr012/06tr012.html>; Internet; accessed 14 December 2006.

Clements, Paul, Kazman, Rick, and Klein, Mark. 2000. *ATAM: Method for Architecture Evaluation*. (2000). Carnegie Mellon: Software Engineering Institute.

Clements, Paul, Kazman, Rick, and Klein, Mark. 2002. *Evaluating Software Architectures: Methods and Case Studies*. (2002).SEI Series in Software Engineering.

Commander Fleet Forces Command (Commander, Fleet Forces Command) Norfolk, VA Naval Message, Subject: 221414Z OCT 03, RQMT FOR STANDARD NAVY REGIONAL ENTERPRISE MESSAGING SOLUTION, UNCLASSIFIED 221414Z October 2003.

Commander Naval Network Warfare Command (ALCOM 029-04) (COMNAVNETWARCOM) Norfolk, VA Naval Message, Subject: 101644Z MAY 04, DEFENSE MESSAGE SYSTEM (DMS) NMCI CLIN 21 GUIDANCE (ALCOM 029-04), UNCLASSIFIED 101644Z May 2004.

Commander Naval Network Warfare Command (COMNAVNETWARCOM) Norfolk, VA Naval Message, Subject: 152158Z DEC 04, NAVY TACTICAL COMMUNICATIONS DEVELOPMENT MESSAGE-1, UNCLASSIFIED 152158Z Dec 04.

Conner, Daryl R. *Managing at the Speed of Change*. New York: Villard Books, 1992.

Defense Information Systems Agency, Defense Message System Overview, Arlington, Virginia. (1998).

Delizo, Robert, SPAWAR PMW 160.3. 2005. *Background paper on Navy Regional Enterprise Messaging System (NREMS)*. (2005).

Delizo, Robert, SPAWAR PMW 160.3. 2005. *Navy Regional Messaging System (NREMS) Program Status Presentation*. (12 Feb 200).

Jick, Todd D. *Managing Change: Cases and Concepts*. Homewood, IL: Irwin, 1993.

Kirkpatrick, Donald L. *How to Manage Change Effectively*. San Francisco: Jossey-Bass, 1985.

Lockheed Martin Corporation (LMC). 2004. *(SDA) Defense Message System (DMS) Recommended System Design Architecture (SDA) Document Release 3.0 (Update)*. (2004) Manassas, VA.

Milton, John W., Defense Information Systems Agency (DISA). 2005. *Defense Message System Proxy User Agent Policy Implementation Instruction, Interim Procedure 34-V01*. Washington, D.C. (2005).

National Communications System (NCS). 2000. *Adopting the Defense Message System (DMS): A Guidebook for the Office of the Manager National Communications System*. Contract Number DCA 100-95-C-0113. (2000).

Program Executive Officer (PEO) C4I and Space PMW-160. 2005. *FY06 Project Definition Document (PDD) for Naval Regional Messaging System (NREMS) (PMW 160): in support of Tactical Switching Program (PMW 790): (PMW 160) in support of Tactical Switching Program*. (2005). San Diego: SPAWARSYSCEN.

Program Executive Officer (PEO) C4I and Space PMW-160.3. 2007. *Navy Regional Enterprise Message System (NREMS) Program Status*. San Diego: SPAWARSYSCEN.

Shirey, Robert W. 1993. *The Defense Message System*. (1993). McLean, VA: Mitre Corporation.

SPAWAR Naval Messaging Lab (NML). 2006. (CONOPS) *SPAWAR Naval Messaging Lab, Concept of Operations (CONOPS) Navy Regional Enterprise Message System (NREMS): Yokosuka Pilot*. (2006) San Diego: Program Executive Office C4I and Space PMW 160.3.

SPAWAR PMW-166,. 2004. *Navy Automated Message Handling System (AMHS) Operational Concept Document (OCD) and Architectural Outline*, 25 June 2004. San Diego, CA.

U.S. Department of Defense. (DODIG) Department of Defense Office of the Inspector General (DODIG). (2003). *Information Technology Management: Transition from the Automatic Digital Network to the Defense Message System (D-2003-075)*. <http://www.dodig.osd.mil/audit/reports>; Internet; accessed 23 July 2006.

U.S. Department of Defense. (MROC) Defense Information Systems Agency. 1997. *Multicommand Required Operational Capability (MROC) Change 2*. Washington, D.C. (1997).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Commanding Officer
ATTN: Kathleen Grauer (PMW 160.3, Principal APM)
Space and Naval Warfare Systems Center
San Diego, California
4. Commanding Officer
Naval School, Civil Engineer Corps Officers
Naval Construction Battalion Center
Port Hueneme, California
5. Professor Dan Boger
Naval Postgraduate School
Monterey, California