April 8, 2003

Information Technology Management

Transition From the Automatic Digital Network to the Defense Message System
(D-2003-075)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at http://www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AUTODIN	Automatic Digital Network
DCID	Director of Central Intelligence Directive
DISA	Defense Information Systems Agency
DMS	Defense Message System
DSA	Directory System Agent
EAM	Emergency Action Message
FCD	Functional Content Document
IC	Intelligence Community
JITC	Joint Interoperability Test Command
MAISRC	Major Automated Information System Review Council
MROC	Multicommand Required Operational Capability
NIPRNET	Non-Secure Internet Protocol Router Network
OASD(C3I)	Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
SIPRNET	Secret Internet Protocol Router Network
VPN	Virtual Private Network

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

April 8, 2003

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
DIRECTOR, JOINT STAFF

SUBJECT: Report on the Transition From the Automatic Digital Network to the Defense Message System (Report No. D-2003-075)

We are providing this report for review and comment. We conducted this audit in response to a congressional request.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) did not provide comments and comments from the Director, Joint Staff were received too late to be considered in preparing the final report. Therefore, we request that the Assistant Secretary of Defense provide comments by May 8, 2003. If the Director, Joint Staff does not submit additional comments by May 8, 2003, we will consider the comments received as the response to the final report.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to Audls@dodig.osd.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the Secret Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Mr. Donald A. Bloomer at (703) 604-8863 (DSN 664-8863). See Appendix D for the report distribution. The team members are listed on the inside back cover of this report.

Thomas F. Gimble
for David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General of the Department of Defense

Report No. D-2003-075 **April 8, 2003**
(Project No. D2002LA-0109)

Transition From the Automatic Digital Network to the Defense Message System

Executive Summary

Who Should Read This Report and Why? This report should be read by personnel involved with managing the Defense Message System (DMS), as well as those who manage the development of information technology systems. This report addresses DMS user requirements and intelligence community directory security.

Background. The Automatic Digital Network (AUTODIN) was implemented in 1962 to provide DoD secure and reliable messaging capability. However, after a study conducted in the late 1980s revealed that AUTODIN was costing in excess of $700 million per year to operate, a search for a replacement messaging system began. The Defense Information Systems Agency started developing DMS in 1988 to replace the messaging functions provided by AUTODIN and other legacy electronic mail systems. In order to acquire the DMS products and services needed, the Air Force awarded a contract to Loral Federal Systems Company in 1995. As of September 30, 2002, DoD had expended about $9 billion in total program costs (FY 1990 through FY 2002) in support of DMS. Those costs include investment costs of $2.29 billion, operations and support costs of $0.15 billion, and legacy (AUTODIN) phase-out costs of $6.65 billion. DMS is to be used by all DoD supporting agencies and users to satisfy organizational messaging needs. DMS Release 3.0, the final version, was fielded in June 2002 with an April 2003 operational date and should meet all established user requirements except for emergency action messaging needs and the intelligence community requirements. DoD plans to cease using AUTODIN and close the DMS Transition Hubs by September 30, 2003.

In January 2002, the House Subcommittee on Military Readiness, Committee on Armed Services requested that the Inspector General of the Department of Defense provide an update to the IG DoD Report No. 98-150, "Readiness of the Defense Message System to Replace the Automatic Digital Network," June 11, 1998. Specifically, the audit was to review and evaluate the development, fielding, and cost of DMS.

Results. Although DMS Release 2.2 did not meet all user and security requirements, DMS Release 3.0 and proposed alternatives to meet intelligence community requirements should satisfy all Multicommand Required Operational Capability and security requirements. Although DMS Release 3.0 should satisfy all Multicommand Required Operational Capability requirements, DMS Release 2.2 did not meet all user requirements, such as message delivery, non-delivery notices, and directory information, and was not widely used. Because of inadequate guidance and oversight, DMS implementation was not on schedule and planned savings of $453 million had not been realized. However, in order to move forward, DMS Release 3.0 should be allowed to operate, and given appropriate support, for a reasonable amount of time to determine whether it can meet user requirements. If DMS does not meet user requirements, then a survey should be conducted and a working group established to develop a solution to satisfy user requirements (finding A).

DMS Release 3.0 does not satisfy intelligence community requirements for directory security. As a result, the intelligence community may not have a secure permanent messaging system available to meet its requirements by the DMS Transition Hub closure date of September 30, 2003. Because the Defense Information Systems Agency and the intelligence community have agreed on a solution to address the directory security requirements, this report makes no recommendations (finding B).

Management Comments. A draft of this report was issued on March 14, 2003. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) did not provide comments and comments from the Director, Joint Staff were received too late to be considered in preparing the final report. Therefore, we request that the Assistant Secretary of Defense provide comments by May 8, 2003. If the Director, Joint Staff does not submit additional comments by May 8, 2003, we will consider the comments received as the response to the final report.

Table of Contents

Background

In January 2002, the Chairman of the House Subcommittee on Military Readiness, Committee on Armed Services requested that the Inspector General of the Department of Defense provide an update to the IG DoD Report No. 98-150, "Readiness of the Defense Message System to Replace the Automatic Digital Network," June 11, 1998 (see Appendix B).

Automatic Digital Network. AUTODIN was developed as a messaging network in the late 1950s with initial implementation in 1962. AUTODIN was to provide DoD secure and reliable transmission of organizational messages. A study conducted in the late 1980s revealed that AUTODIN was costing in excess of $700 million per year to operate. As a result, the Defense Information Systems Agency (DISA) started developing DMS in 1988 to replace the messaging functions provided by AUTODIN and other legacy electronic mail (e-mail) systems. In order to acquire the DMS products and services needed, the Air Force awarded a contract to Loral Federal Systems Company[1] in 1995. The contract had a 2-year base period and six option years, with an estimated value of $1.7 billion (total value over the 8-year period). Option Period Six of the contract extended the performance period from May 1, 2002, through April 30, 2003. DoD planned to cease use of AUTODIN by September 30, 2003. The DMS Transition Hubs that allow DoD Components to transmit messages using AUTODIN are scheduled for closure on that date.

Defense Message System. DMS is a messaging mail system based on commercial off-the-shelf software that provides a flexible messaging capability. DMS was designed to perform multimedia messaging (for example, text and graphics) and directory services. Directory services provide a means to locate computer systems, files, individuals, and e-mail addresses and to perform other lookup requirements. DMS takes advantage of the underlying Defense information infrastructure and security services. DMS provides access to messaging services for all DoD users worldwide (including deployed tactical users) as well as an interface to other U.S. Government agencies, allies, and Defense contractors. DMS relies on current and emerging technological capabilities to provide secure organization-to-organization and individual messaging services. DMS is also intended to have the capability of handling all classification levels of information, from Unclassified to Top Secret, including classification levels used by the intelligence community (IC).[2] Before fielding a DMS release, the Joint Interoperability Test Command (JITC) tests it for operability. Although DMS Release 3.0 was fielded in June 2002 (with an operational date of April 2003), as of November 2002, DMS Release 2.2 was the most current version in use. DMS is expected to reach full operational capability by FY 2008 through a series of software releases. DMS Release 3.0 is expected to satisfy Multicommand Required Operational Capability (MROC) requirements (listed in Appendix C).

[1] Loral Federal Systems Company was acquired by Lockheed Martin Corporation in April 1996.

[2] The IC comprises 14 Government agencies and organizations, including the Central Intelligence Agency, the Defense Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency, which carry out the intelligence activities of the U.S. Government.

Roles and Responsibilities. The key players in the implementation of DMS are the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (OASD[C3I]), the Joint Staff, DISA, and the Services.

OASD(C3I) is the designated milestone decision authority for DMS and is responsible for providing programmatic policy and acquisition guidance and oversight for DMS. The Joint Staff is responsible for reviewing DMS actions for consistency with validated requirements; ensuring adequate coordination with and validating requirements from the combatant commands and the Services; and providing joint doctrine as required. DISA is responsible for maintaining oversight of DMS acquisition; providing overall operational management and control of DMS; ensuring Joint Staff-validated requirements are met; and coordinating DoD-wide implementation of DMS. The responsibilities of the Services include maintaining aggressive program management during the implementation of DMS; ensuring that the transition planning and AUTODIN phase-out planning[3] are up-to-date, executed on schedule, and consistent with overall program milestones; providing operational support for the management of assigned DMS components in accordance with approved DMS operational policy and procedures; and maintaining adequate training in accordance with the DMS training plan.

The Services and the Defense agencies reached a consensus in 1989 to modernize DoD messaging by replacing the legacy message systems with DMS. To accomplish the modernization of DoD messaging, DISA and the Military Departments established DMS program management offices. An agreement reached between DISA and the Military Departments stipulated that DISA would provide all required infrastructure and software products and that the cost of fielding the hardware products would be shared. The Military Departments and the Defense agencies would be responsible for DMS implementation throughout their respective organizations.

Messaging Requirements. In 1989, the Joint Staff validated MROC 3-88, which outlined the requirements to be met by DMS. In 1994, DISA developed and the Joint Staff approved change 1 to the "Required Operational Messaging Characteristics," April 15, 1994, that contained more detailed requirements to be met by DMS. In 1997, those requirements were incorporated into MROC 3-88, Change 2 (hereafter referred to as MROC). The MROC serves as the requirements basis for all DMS projects and components, including the Target Architecture and Implementation Strategy, the Concept of Operations, and Allied Communication Publication 123[4] being developed with the support of the Military Communications-Electronics Board.

DMS comprises the hardware, software, procedures, personnel, and facilities required for the electronic delivery of messages between the Services and Defense agencies and for interfaces to the messaging systems of allies and Defense contractors. OASD(C3I) designated DMS as the messaging system to be used for

[3] AUTODIN phase-out planning is the process or plan of action for closure of the DMS Transition Hubs.

[4] Allied Communication Publication 123, "Common Messaging Strategy and Procedures," August 15, 1997, defines the services, protocol, and procedures to support electronic messaging.

DoD and its supporting agencies, thereby initiating the migration from AUTODIN and other legacy message systems to DMS. DISA provided the DMS infrastructure and fielded software in January 1998 with DMS Release 1.1. DMS Release 2.2 was fielded in April 2001. Each release provided enhanced capabilities. DISA fielded DMS Release 3.0 in June 2002 with a scheduled operational date of April 2003.

Acquisition Strategy. The DMS Program was designated as a Major Automated Information System Review Council (MAISRC) acquisition category IA[5] program in March 1994. In July 1998, the MAISRC was disestablished and the Information Technology Overarching Integrated Product Team assumed responsibility for the management oversight of the DMS Program. Milestones set by the MAISRC dictated that DMS be acquired using an evolutionary acquisition[6] approach and be implemented progressively, through a series of DMS releases, with the transition from AUTODIN to DMS first, followed by the capability to provide "unclassified-but-sensitive" messaging and then classified messaging. The full range of DMS operational capabilities would be achieved through coordinated product releases. Each release is focused on a critical aspect of DMS and updates earlier releases that results in enhanced capabilities as part of an integrated system. The fielding of each new release was dependent upon the successful completion of operational testing by JITC.

Cost. As of September 30, 2002, DoD had expended about $9 billion in total program costs (FY 1990 through FY 2002) in support of DMS. Those costs include investment costs of $2.29 billion, operations and support costs of $0.15 billion, and legacy (AUTODIN) phase-out costs of $6.65 billion. In 1998, DoD had envisioned that DMS would save $453 million by shutting down AUTODIN in December 1999. A decrease in original legacy phase-out cost estimates and an increase in DMS cost estimates, as well DoD not meeting the December 1999 deadline, led to a negative return on investment of $266 million over the life of the DMS program (through FY 2013).

Objectives

Our overall audit objective was to determine whether DMS can replace critical AUTODIN messaging capabilities. Specifically, the audit reviewed and evaluated the development, fielding, and cost of DMS. We did not evaluate management controls because the audit was limited to a review of whether DMS as fielded could meet the requirements of users. See Appendix A for a discussion of the scope and methodology and for prior coverage related to the overall objective.

[5] An acquisition category IA program is a Major Automated Information System designated by OASD(C3I) as an automated information system acquisition program. Also, the acquisition program is estimated to require program costs in any single year in excess of $25 million, total program costs in excess of $100 million, or total life-cycle costs in excess of $300 million in FY 1990 constant dollars.

[6] Evolutionary acquisition is an approach that fields an operationally useful and supportable capability in as short as time as possible. It delivers an initial capability with an explicit intent of delivering improved or updated capability in the future.

A. Defense Message System Status

Although DMS Release 3.0 should satisfy all MROC requirements, DMS Release 2.2 did not meet all user requirements and was not widely used because the system was fielded incrementally and OASD(C3I) and the Joint Staff did not provide adequate guidance and oversight of the DMS Program. As a result, DMS may not be able to replace the critical AUTODIN emergency action messaging capability by September 30, 2003, the date DoD plans to cease using AUTODIN and close the DMS Transition Hubs. In addition, DMS was not on schedule and planned savings of $453 million had not been realized.

DMS Multicommand Required Operational Capability

According to the DISA DMS program manager, the results of independent operational assessments and tests by JITC for DMS Releases 1.0 through 3.0 indicate that DMS Release 3.0, scheduled to be operational by April 2003, should satisfy all MROC requirements. DMS was required to meet requirements in 12 areas, listed in Appendix C. Although DMS Release 3.0 was fielded in June 2002, with an operational date of April 2003, as of November 2002, DMS Release 2.2 was the most current version in use. The MROC sets forth DMS messaging requirements for DoD.

DMS Release 2.2 users in operational environments in the European and Pacific theaters encountered problems with message delivery, non-delivery notices, and the directory while operating DMS Release 2.2. In addition, JITC conducted operational assessments or tests of DMS to determine the extent to which each DMS release was operationally effective and operationally suitable to support DoD organizational messaging requirements. Those assessments or tests revealed that DMS Release 2.2 did not meet MROC requirements for confidentiality/security, integrity, and availability/reliability. Lastly, DMS did not support strategic messaging requirements, specifically emergency action messages (EAMs).

DMS Performance

This section discusses the performance of DMS, including concerns of users in the European and Pacific theaters about message delivery, the directory, and emergency action messaging in operational environments.

Message Delivery and Non-Delivery Notices. A JITC operational assessment showed that DMS Release 2.2 was unable to provide the capability to trace messages from the writer to the reader (message delivery). In addition to DMS Release 2.2 not meeting the MROC requirement for message delivery, DMS users experienced problems with non-delivery notices.

DMS users experienced a high number of non-delivery notices. The MROC states that DMS must deliver messages to intended recipients with a high degree of certainty. To measure the performance of DMS, DISA established a threshold of 3 percent for non-delivery of messages. DISA monitored message delivery performance on a monthly basis and reported that during the month of August 2002 DISA and the Services sent out 266,421 messages and received non-delivery notices for 18,958 (7 percent) of the messages, more than double the DISA-established acceptable rate. The Services encountered non-delivery notice rates ranging from 5.5 percent to 11 percent for the period of April through July 2002. During that 4-month period the percent of messages not delivered, generating a non-delivery notice, increased from 7.9 percent to 8.1 percent for the Army, from 6 percent to 9 percent for the Air Force, and from 8.9 percent to 11 percent for the Marine Corps. Navy non-delivery notices decreased from 8 percent to 6.1 percent during the same period. Each of the Services experienced non-delivery rates above the established 3 percent threshold. The non-delivery notices occurred because of expired, incorrect, or invalid addresses; misrouting of messages in the DMS backbone;[7] or improperly configured DMS components and profiles. DMS non-delivery notices did not provide an explanation as to why the message did not go through or provide a solution to correct the problem. Non-delivery notices required the sender to do additional followup work to ensure that the information was received by the intended organization. In addition, message originators did not know whether messages reached their intended recipients.

We conducted panel discussions with groups of DMS users at organizations in the European and Pacific theaters. Personnel at those panel discussions provided us details of their message delivery problems.

Army. Army personnel at panel discussions in the European and Pacific theaters stated that they experienced problems with non-delivery notices and message delivery. In the European theater, Army users stated that non-delivery notices did not clearly explain why the message did not go through, offer suggestions for correction, or provide any detailed information about the problem. In the Pacific theater, personnel at the U.S. Army Pacific, Command Center, stated that the majority of their delivery problems dealt with receiving delivery confirmation notices on DMS messages that they had sent but later discovering the messages had not reached the intended recipients.

Navy. Panel discussions with Navy personnel in the European and Pacific theaters revealed that Navy DMS users experienced problems with message delivery. For example, an official at a transportation office in Europe and a Fleet Industrial Support Center official in the Pacific theater stated that DMS messages were not always delivered to their customers. As a result, they used the Secret Internet Protocol Router Network (SIPRNET)[8] to meet part of their messaging needs. Personnel from the Naval Pacific Meteorology and Oceanography Facility, which provides weather information to ships and pilots, stated that they experienced instances where weather condition messages did not reach the facility's customers.

[7] The Defense Information Systems Network is the worldwide backbone router system for the Defense information infrastructure.

[8] The SIPRNET is the Secret portion of the Defense Information Systems Network.

Air Force. Air Force personnel in the European and Pacific theaters experienced problems with non-delivery notices and message delivery. Panel discussions with Air Force DMS users in the European theater identified that the Air Force Air Mobility Operations Control Center (the Control Center), located at Ramstein Air Force Base, Germany, could not routinely determine from non-delivery notices which recipient had not received a message, or how to correct the problem. An official in the Control Center stated that about one-third of the DMS messages sent did not reach their destinations. The Control Center is responsible for planning, scheduling, tasking, and executing theater air mobility. When executing Joint missions, it is imperative that Control Center messages reach their intended destinations in a timely manner. Panel discussions with DMS users in the Pacific theater identified that the Pacific Operations Support Command (the Support Command), located at Hickam Air Force Base, Hawaii, also experienced problems with high-importance DMS messages not reaching their destinations. The Support Command is responsible for command and control of the nine air wings within the Pacific theater and must have assured means of communications. Some of the non-delivery notices the Support Command received were for messages sent to airfields; however, the non-delivery notices did not provide an explanation as to why the messages did not go through. Many of those locations were not DMS-capable and required that the messages be transmitted by AUTODIN or secure fax. The Support Command allocated additional time to complete followup calls to all locations to determine which locations received the messages, and then find an alternative way to transmit to those that had not received the messages.

Overall, to ensure that messages would be delivered to intended recipients, DMS Release 2.2 users relied on other means, including AUTODIN, non-DMS e-mail, facsimile transmissions, the Global Command and Control System,[9] the Joint Operation Planning and Execution System,[10] the Non-Secure Internet Protocol Router Network (NIPRNET),[11] and the SIPRNET.

Directory. DMS Release 2.2 users in both the European and Pacific theaters found that navigating the directory system was a time-consuming and daunting task. The directory system within DMS stores recipients' addresses, security-related information, and information necessary to provide organizational and individual messaging on a global basis. The DMS directory system stores information in a distributed, hierarchical structure known as the Directory Information Tree. The Directory Information Tree structure was not standardized among and within the Services, making it extremely difficult to navigate making tasks such as finding DMS addresses time consuming. The absence of a standardized structure for information in the DMS directory required users to be familiar with the naming convention used by each organization to establish its directory in order to find addresses in a timely manner. Master Key Plus, a DMS tool used to find DMS organizational addresses and store those addresses in user contact lists, was available for DMS Release 2.2; however, the user had to

[9] The DoD computerized system of record for strategic command and control functions.

[10] An integrated, joint conventional command and control system used by senior-level decision makers and their staffs to plan and conduct joint military operations.

[11] The NIPRNET is the non-secure, common-user portion of the Defense Information Systems Network.

download Master Key Plus software. Master Key Plus is included in DMS Release 3.0 and should meet user needs.

JITC Assessments of DMS. According to the results of operational tests or assessments conducted by JITC, DMS Release 2.2 did not fully meet four of the 12 MROC requirements. A complete list of all 12 MROC requirements is listed in Appendix C.

Confidentiality/Security. A JITC operational assessment showed that DMS Release 2.2 was unable to provide the capability to process and protect all unclassified, classified, and sensitive messages at their appropriate security levels. That capability includes writer-to-reader message confidentiality; support for appropriate message security levels and markings; and authentication, access management, and access control using approved security mechanisms. However, according to another JITC operational assessment, DMS Release 3.0 should satisfy the MROC requirement.

Message Delivery. A JITC operational assessment showed that DMS Release 2.2 was unable to deliver messages to the intended recipients with a high degree of certainty. The system was not able to provide traceability from writer to reader. However, according to another JITC operational assessment, DMS Release 3.0 should satisfy the MROC requirement.

Integrity. A JITC operational assessment showed that DMS Release 2.2 was unable to provide system-level safeguards against accidental, unauthorized, or malicious actions that could result in the alteration of security protection mechanisms, security classification levels, addressing or routing information, and audit information. However, according to another JITC operational assessment, DMS Release 3.0 should satisfy the MROC requirement.

Availability/Reliability. A JITC operational assessment showed that DMS Release 2.2 was unable to provide the appropriate safeguards to protect the system from accidental, unauthorized, or hostile actions, resulting in the inability to use system services. However, according to another JITC operational assessment, DMS Release 3.0 should satisfy the MROC requirement.

DMS Support of Emergency Action Messages (EAMs). According to DISA and the U.S. Strategic Command, located at Offutt Air Force Base, Nebraska, DMS cannot support all strategic messaging requirements, such as EAMs.[12] The inability of DMS to support EAMs was identified as a potential problem in 1997 when an analysis indicated that DMS could not fully support the dissemination of EAMs in accordance with Chairman of the Joint Chiefs of Staff Instructions 5119.01[13] and 6811.01, "Nuclear Command and Control System

[12] Previously reported in the Office of the Inspector General of the Department of Defense Report No. 98-150, "Readiness of the Defense Message System to Replace the Automatic Digital Network," June 11, 1998.

[13] Chairman of the Joint Chiefs of Staff Instruction 5119.01, dated December 5, 1994, was canceled June 9, 2000, and replaced by Chairman of the Joint Chiefs of Staff Instruction 5119.0 1A, "Charter for the Centralized Direction, Management, Operation, and Technical Support of the Nuclear Command, Control, and Communication System," June 9, 2000.

Technical Performance Criteria," January 10, 1994. In September 1997, the Joint Staff acknowledged that DMS would not fully support the requirement to disseminate EAMs formerly satisfied by AUTODIN.

Extensive efforts to address the issue culminated in the development of an interim plan to use the DMS Transition Hubs until another solution was determined. The 1999 Defense Planning Guidance directed the Joint Staff to lead a Nuclear Command, Control, and Communications Integrated Product Team to identify requirements; develop a concept of operations; and prototype, implement, and test a second interim solution, the hybrid solution, for disseminating EAMs before the DMS Transition Hub closure date. The Military Communications-Electronics Board (the Board) granted the formal endorsement of the EAM Hybrid Interim Solution on November 29, 2000. In June 2001, the Board established an EAM Board of Directors to test and monitor the EAM Hybrid Interim Solution's progress and address any unresolved issues. In addition, the EAM Board of Directors will monitor the development of a long-term follow-on solution.

Problem Resolution. The problems DMS users experienced with message delivery, non-delivery notices, and the Directory Information Tree were not significant. With appropriate guidance, experience, and the issuance of Master Key Plus with DMS Release 3.0, those problems should be resolved. DMS Release 3.0 should satisfy all of the MROC requirements, including those only partly met by DMS Release 2.2. In addition, EAM support was being addressed by both short-term and long-term resolutions.

Limited Use of DMS. DMS implementation did not appear to be a priority at most sites visited in the European and Pacific theaters. Site visits revealed that some users had not received any formal training on the system, did not understand the intent of the system, or why or when to use DMS. At the sites, units had DMS installed but personnel had not been trained on it or its application. Overall, not only was DMS not widely used, it had also developed a negative reputation due to the lack of the system's original capabilities and a lack of user training and education on the system.

Resolution of User Concerns. According to the results of a JITC assessment, the message delivery and the directory problems encountered by DMS users in the European and Pacific theaters should be resolved when DMS Release 3.0 is put into use in April 2003. Once DMS Release 3.0 is put into use and allowed to operate for a reasonable amount of time, users should be surveyed to determine whether DMS Release 3.0 meets all user and MROC requirements. If required, a working group should be established to develop a solution to satisfy user requirements.

DMS Fielding and Program Oversight

DMS Release 2.2 did not meet user needs and was not widely used because DMS was fielded incrementally and OASD(C3I) and the Joint Staff did not provide adequate guidance or oversight of the DMS Program.

Incremental Fielding. DoD users encountered problems because DMS was fielded before it was mature enough to fully support user needs. DMS Releases 1.0 and 2.1, although tested before fielding, lacked the capability to support most units' basic missions; therefore, the combatant commands and the Services did not mandate that subordinate units use DMS. As a result, the implementation of the system may have been adversely affected by incrementally fielding DMS.

Adequacy of Guidance and Oversight. OASD(C3I) did not provide adequate guidance and oversight for the implementation and usage of DMS. DMS was not widely used among operational units in the European and Pacific theaters because of incremental implementation; poor measurement criteria; and insufficient command emphasis requiring use of DMS once fielded. The Joint Staff needs to ensure that the Services provide sufficient command emphasis on the DMS Program.

Incremental Implementation. The DMS Product Plan (Version 3.03), dated August 20, 1999, envisioned an organizational messaging transition from AUTODIN to DMS by the end of December 1999. However, DMS site implementation problems prevented that goal from coming to fruition. A December 28, 1999, memorandum from OASD(C3I) stated, "operational issues warrant a re-look at the overall AUTODIN to DMS transition plan." The memorandum goes on to state:

> It's now clear some of the CINCs [commanders in chief, now referred to as combatant commanders], Services, and DoD Agencies are unable to meet [the established] deadline. While many DMS organizational accounts should be functional by December 1999, DMS integration into operational business practices will not be sufficiently mature to replace AUTODIN for organizational messaging.

Site implementation processes continued to be a problem for later DMS releases. A July 1, 2002, memorandum from OASD(C3I) states:

> Site implementation processes and procedures, including training, were identified in the OT [operational test] as needing improvement. DISA, in coordination with the Services, shall re-examine the OT results to identify common site implementation problems and determine if adjustment to the DMS site implementation guidance is required.

As cited above, OASD(C3I) recognized that improvements to the site implementation guidance were required. We believe OASD(C3I) should monitor DMS site implementation processes and procedures to ensure that DMS is implemented in the combatant commands and Services in the most efficient and effective manner.

Measurement of DMS Usage. On December 28, 1999, OASD(C3I) issued a revised transition plan. The plan focused on increasing DMS use by monitoring the transition progress in a DISA monthly report. The revised transition plan also established a deadline of September 15, 2000, for all organizational accounts of combatant commands, Services, and Defense agencies to be operational (no longer sending AUTODIN messages) and all of the general service message traffic to be transitioned to DMS. However, the measurement criteria used in the plan was not quantifiable enough to determine whether the users were fully using the system's capabilities to support their mission requirements.

Operational Versus Functional Use of DMS. The revised transition plan established the terms "Functional" and "Operational"[14] to distinguish whether units had completed the transition from AUTODIN to DMS. However, use of those terms did not mean a unit actually used DMS. Units could have DMS capability (functional) and stop using AUTODIN (operational) without using DMS to meet their messaging needs by using other systems instead of DMS. For example, users in both the European and Pacific theaters stated their units were DMS functional and operational even though they only used DMS to send test messages. Other units in the Pacific theater reported being DMS functional and operational even though personnel in those units did not know which computer contained the DMS software. Personnel at those units stated that the majority of their message traffic was sent using other systems, such as non-DMS e-mail, facsimile transmissions, the Global Command and Control System, the Joint Operation Planning and Execution System, NIPRNET, and SIPRNET. OASD(C3I) and Joint Staff guidance should have mandated DMS usage after implementation.

Revised Measurement of DMS Usage. On April 12, 2001, OASD(C3I) issued another revision to the transition plan that established new milestones, modified the definition of operational, and provided additional clarity regarding the applicability of DMS[15] and the use of non-DMS means to support organizational messaging. The guidance also stated that non-DMS means of supporting organizational messaging would only be considered for approval if DMS could not support validated user requirements. However, the revised transition plan did not establish a method to verify the usage of DMS in an operational environment. We believe that OASD(C3I) should direct that each site conduct a message traffic analysis to determine whether key organizational messages, such as those related to budgeting, command position, and troop movement, were sent on DMS.

Command Emphasis. The Joint Staff did not provide adequate guidance and oversight to ensure that the Services provided command emphasis on the DMS Program. A Joint Staff official recognized that additional emphasis was required from the Joint Staff and the Services to get the system fully operational. Despite having already missed two DoD-mandated deadlines, several units in the European and Pacific theaters were not prepared to fully transition to DMS. The Army Chief Information Officer stated in a May 31, 2002, message to Army users that there was concern that the transition from AUTODIN to DMS was again not occurring at a rate to "meet AUTODIN closure." He stated that the Army program manager for DMS needed commanders' help and assistance to ensure that Army commands were ready to meet the DoD deadline. In order to provide

[14] Functional was defined as when a unit had the ability to send and receive signed and encrypted DMS messages. Operational was defined as when a unit was no longer sending AUTODIN messages.

[15] Under the modified definition of "operational," an account was operational when all of the organization's messages were released from, and received at its DMS organizational account.

emphasis on DMS, the Chief Information Officer established an Army deadline for Army-wide organizational messaging to be fully transitioned to DMS by March 1, 2003. As of March 5, 2003, that deadline had not been met.

The Air Force experienced similar problems. Despite monthly reports from the European and Pacific theaters that more than 95 percent of all organizational accounts were both operational and functional, Air Force units we visited in those theaters did not use DMS for all of their messaging needs and users had limited knowledge of the intent of the system. We believe that increased command emphasis by the Joint Staff and the Services on the benefits of DMS would have allowed users to understand the system better and the users would, in turn, have used DMS more.

Impact on DMS Use

Although DMS Release 3.0 should satisfy all MROC requirements, it may not be able to replace the critical AUTODIN emergency action messaging capability by September 30, 2003, the closure of the DMS Transition Hubs. DoD has expended more than 13 years of effort and spent about $9 billion in total program costs on DMS and legacy systems. In addition, DoD will not be able to realize the initial planned savings of $453 million. Instead, it will incur a negative return on investment of at least $266 million for general service messaging capabilities over the life of the DMS Program through FY 2013. Lastly, according to a DISA official, the DMS Program plans additional expenditures of almost $5 billion. The planned expenditures consist of investment costs, operations and support costs, and legacy phase-out costs through FY 2013.

Recommendations

A.1. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence):

a. Resolve user problems with message delivery, non-delivery notices, and the Directory Information Tree.

b. Allow Defense Message System Release 3.0 to operate for a reasonable amount of time after the closure of the Defense Message System Transition Hubs on September 30, 2003, to validate whether the Defense Message System can meet all Multicommand Required Operational Capability and user requirements.

c. If the Defense Message System does not meet user requirements, conduct a survey to identify messaging requirements that are not being met and establish a working group to develop a solution to satisfy user requirements.

d. Direct that each site conduct a message traffic analysis to determine whether key organizational messages, such as those related to budgeting, command position, and troop movement, are being sent on DMS.

A.2. We recommend that the Director, Joint Staff issue policy and guidance requiring the combatant commands, the Services, and the DoD agencies to:

a. Conduct a message traffic analysis to determine how the Defense Message System can best support organizational messaging needs.

b. Use the Defense Message System to satisfy those organizational messaging needs identified in Recommendation A.2.a. after its implementation.

c. Ensure that the Services provide command emphasis on the Defense Message System Program, to include explaining the intent and nature of operations of the system and educating users on the benefits of the system.

Management Comments Required

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) did not provide comments and comments from the Director, Joint Staff were received too late to be considered in preparing the final report. Therefore, we request that the Assistant Secretary of Defense provide comments in response to the final report. If the Director, Joint Staff does not submit additional comments, we will consider the comments received as the response to the final report.

B. Intelligence Community Directory Security

DMS Release 3.0 does not satisfy IC requirements for directory security because DISA was not able to develop a directory architecture that met critical IC directory security requirements. As a result, the IC may not have a secure permanent messaging system available to meet its requirements by September 30, 2003.

Criteria

IC Requirements. The overall IC DMS requirements were first published in "Intelligence Community Defense Message (DMS) Requirements, Version 1.1," April 29, 1998. In addition, a list of IC Priority 1 requirements were published in the "Intelligence Community (IC) Requirements & Analysis Report" (the Analysis Report), July 15, 1998, and later in the "DMS Release 3.0 IC Priority 1 Requirements Implementation Matrix," January 7, 2000. Priority 1 requirements are those designated by the IC as most critical, including directory security requirements, which must be met before the IC will implement DMS.

Director of Central Intelligence Directive (DCID). DCID 6/3, "Protecting of Sensitive Compartmented Information within Information Systems," June 5, 1999, sets out the security policies and requirements for information systems in the IC. DMS directory security must comply with the provisions of DCID 6/3 in order to successfully satisfy IC requirements. On June 26, 2002, OASD(C3I) determined that DCID 6/3 should be used as the standard to ensure IC DMS directory security requirements are met.

According to the Directory Security Functional Content Document (FCD), "DMS Release 3.0 Directory Security: Consolidated General Service/IC DMS Directory Security Requirements (DCID 6/3 extract)," October 25, 2002, the DMS Release 3.0 directory does not meet 10 of the DCID 6/3 requirements regarding directory security. The DISA DMS Program Management Office and Lockheed Martin Corporation prepared the FCD to document the problems with directory security. Table 1 lists the 10 unmet DCID 6/3 requirements identified by the FCD.

Table 1. Unmet DCID 6/3 Directory Security Requirements

	DCID 6/3 Requirement	Description
1	4.B.2.a(2)	Access control, including a discretionary access control policy.
2	4.B.2.a(4)(d)(3)	Activities at the system console (either physical or logistical consoles), and other system-level accesses by privileged users.
3	4.B.2.a(8)	Identification and Authentication.
4	4.B.4.a(13)	Identification and Authentication.
5	4.B.4.a(14)(a)	Implementation and support of a trusted communications path between the user and the Security Support Structure of the desktop for login and authentication.
6	4.B.4.a(14)(b)	In the case of communication between two or more systems (e.g. client-server architecture), bi-directional authentication between the two systems.
7	4.B.2.a(17)(d)[5]	Information encrypted using NSA-approved encryption mechanisms appropriate for the classification of stored data.
8	5.B.3.a(7)	Data and software storage integrity protection, including the use of strong integrity mechanisms (e.g. integrity locks, encryption).
9	5.B.3.a(11)(a)	Integrity mechanisms adequate to assure the integrity of all transmitted information (including labels and security parameters).
10	5.B.3.a(11)(b)	Mechanisms to detect or prevent the hijacking of a communication session (e.g. encrypted communication channels).

Source: FCD

The overall IC requirements and the list of Priority 1 requirements are broadly defined principles that DMS will be required to meet. DCID 6/3 provides the road map of detailed security steps to follow to ensure the DMS directory satisfies the overall IC requirements.

Directory Security

DMS Release 3.0, the first release to be considered for implementation in the IC, does not satisfy IC requirements for directory security. If directory security requirements, which are Priority 1 requirements, are not met, the IC will not implement DMS. Since the IC requirements were first established in 1998, DISA has considered different solutions to satisfy directory security requirements. As of November 18, 2002, directory security was the biggest unresolved issue facing DMS.

The architecture of the DMS directory of user addresses consists of individual, local directories (Directory System Agents [DSAs]) that contain part of the X.500 directory. X.500 is an international specification established for directory services that defines the mechanisms to support geographically dispersed directories (distributed environments) and to control access to the information stored in the directories.

OASD(C3I) Memorandum. According to the OASD(C3I) memorandum, "DMS Directory Security Requirements," June 26, 2002, effective directory security requires four elements:

- integrity of the directory,
- strong identification and authentication of changes to the directory,
- integrity of directory data, and
- an ability to provide a comprehensive audit of directory changes.

The memorandum states that the DISA Virtual Private Network (VPN) solution to directory security, which was in effect at the time of the memorandum, was inadequate. Specifically, under the VPN solution, boundaries were not well protected and identification and authentication within the VPN was weak (for example, passwords used in DMS were inadequately protected).

Directory Security Functional Content Document. The FCD sets out the shortfalls in the directory architecture of DMS Release 3.0, which features the VPN solution. The FCD also describes the enhancements to be made as part of a phased solution to ensure the DMS directory meets DCID 6/3 requirements.

The DMS directory architecture consists of X.500 DSAs located in a DISA-operated infrastructure as well as in locally operated Service and Defense agency sites. The FCD states that because the directory architecture is widely dispersed, data is transmitted between DSAs. Data transmissions include writes[16] and reads[17] of data between DSAs. In addition, other components, such as DMS messaging clients and tools, connect to DSAs to send or retrieve data.

Despite the fact that DSAs and components are protected by firewalls and there is a global VPN that protects many of the transmissions between DSAs, the FCD notes that much of the directory data is transmitted over unprotected network links, both internal and external. Thus, states the FCD, directory data transmissions are unprotected for significant portions of their travel across the DMS directory architecture.

According to the FCD, DMS Release 3.0, which includes the VPN solution, does not address concerns about the integrity of the directory. It is not possible to update the DMS directory data or configuration without authorization (gained through inputting an identification and password); however, anyone with access to the network (an internal user) can potentially intercept that information in transit. If the intercepted data includes an administrator's identification and password combination, the interceptor could potentially gain access to the authorizations held by that administrator. In order to prevent the risk of interception, the FCD states that all transmissions of directory data must be encrypted.

[16] Directory modifications by authorized system administrators.

[17] Users accessing or reading directory data.

The FCD notes that as long as identifications and passwords are the means of authentication, the DMS directory is vulnerable to unauthorized access if an identification and password are guessed correctly. According to the FCD, the DISA phased solution to address IC DMS directory security requirements will use certificates and a public key infrastructure to authenticate users. That design requires that an imposter gain access to a user's certificate, the user's private key, and the personal identification number used to access the private key in order to impersonate that user. Gaining access to all three of those components is much more difficult than simply guessing a user's identification and password.

Development of the DMS Directory

DISA was unable to develop a DMS directory architecture that met critical IC directory security requirements. The DISA DMS Program Management Office is responsible for developing a solution that satisfies the IC directory security requirements.

The IC requirements for directory security have been well known for several years. The IC released its official DMS requirements, which included directory security requirements, on April 29, 1998. In addition, the IC designated directory security requirements as critical items in its July 15, 1998, and January 7, 2000, DMS Release 3.0 Priority 1 requirements documents. IC DMS Management Office officials stated that they continually reminded the DISA DMS Program Management Office about the criticality of developing an effective solution to the directory security problems. In an effort to address the IC directory security requirements, DISA developed different solutions over the years, including a solution based on FORTEZZA,[18] a VPN solution, and a phased solution.

FORTEZZA-Based Solution. In the 1999 through 2001 timeframe, the DISA DMS Program Management Office considered a FORTEZZA-based solution to meet the IC directory security requirements. According to DISA, the FORTEZZA-based solution never made it past the prototype stage because of development concerns, schedule concerns, and cost. A DISA DMS Program Management Office official indicated that the solution was never formally proposed to the IC.

VPN Solution. The DISA DMS Program Management Office decided in early 2001 to extend a planned VPN implementation to also protect the DMS directory, in place of the FORTEZZA-based solution. The VPN solution was the second solution considered to address IC directory requirements, but it was the first proposed to the IC (in early 2002). However, the Defense Intelligence Communication Accreditation Support Team[19] and the IC did not view the VPN solution as acceptable. During the DMS 3.0 Milestone III decision review

[18] FORTEZZA is a product of the National Security Agency Multi-Level Information System Security Initiative program.

[19] The Defense Intelligence Communication Accreditation Support Team is responsible for analyzing security issues.

process, the Defense Intelligence Communication Accreditation Support Team rejected the VPN solution.

The FCD includes the following major DMS directory security exposures that exist under the DMS Release 3.0 directory architecture, which features the VPN solution:

- transmittal of directory modify requests over unprotected links,
- transmittal of directory data over unprotected links as part of a replication operation,
- vulnerability of a user's identification and password combination to guessing or interception on unprotected links, and
- transmittal of directory data over unprotected links as a result of a read request.

On June 20, 2002, after the VPN solution had been rejected, the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance & Space Systems OIPT tasked the Information Assurance Branch of OASD(C3I) with identifying and clarifying the DoD and IC requirements that would be used to develop a new solution to satisfy IC directory security concerns. The June 26, 2002, OASD(C3I) memorandum established DCID 6/3 as the basis for developing a solution to the directory security problems for both DoD and the IC. The FCD notes that the DISA DMS Program Management Office was to provide a plan of action to develop, test, and implement the directory security requirements established by the OASD(C3I) memorandum.

Phased Solution. On September 19, 2002, DISA presented the Defense Intelligence Communication Accreditation Support Team with a phased solution to the directory security requirements. The team agreed with the approach and the planned schedule. In a memorandum to OASD(C3I), "DMS Directory Security Requirements," November 1, 2002, DISA provided an overview of its plan to complete the directory security enhancements.

Phase one of the phased solution will focus on directory security enhancements critical to achieving DMS Transition Hub closure. According to the DISA memorandum, phase one will include directory write operations, protection of remote directory administration operations, and protection of directory security integrity. In the second phase, DISA plans to address strong authentication for directory read operations and encryption of the directory. According to a DISA DMS Program Management Office official, both phases of the solution would employ Secure Sockets Layer[20] tunnels with bi-directional authentication using DoD or IC public key infrastructure certificates. Directory data in transmission would be encrypted and before the directory could be modified or read, authentication would be required.

[20] Secure Sockets Layer technology is used by digital certificates to encrypt data.

Planned Actions

In order to implement DMS in the IC by the DMS Transition Hub closure date of September 30, 2003, the following actions will need to have been completed:

- development, testing, and fielding of phase one of the DISA phased directory security solution;
- modification and testing of existing DMS components affected by the planned changes to the directory;
- testing of the overall DMS architecture for all IC agencies; and
- approval by the Director of Central Intelligence to implement DMS.

DISA plans to have the phase one solution tested and implemented by the DMS Transition Hub closure date. The directory security shortfalls addressed by phase one are functions that are deemed critical to achieving that closure. As of February 7, 2003, phase one development was ongoing. Phase two, which will complete the directory security enhancements, is projected by DISA to be completed in 2004.

IC officials indicated that the overall IC DMS architecture would undergo a developmental test phase and an operational test and evaluation in the spring of 2003, followed by three additional test phases (including tests of functionality, security, and vulnerability) in June 2003. When the tests are completed, the IC Chief Information Officer will prepare a report summarizing their results. The report will then be presented to the Director of Central Intelligence for review and approval of the entire IC DMS architecture (the core DMS Release 3.0 software product and any supplementary products).

Conclusion

The IC may not have a secure permanent messaging system available to meet its requirements by September 30, 2003. Therefore, IC agencies will have to rely on legacy and existing systems, such as the Joint Worldwide Intelligence Communications System, the IC Bypass,[21] and other forms of secure e-mail, to provide messaging services.

Because DISA had not developed a DMS directory architecture that satisfied IC directory security requirements, a phased solution had to be developed and must be tested and implemented with little room for error prior to the September 30, 2003, deadline. If there are any delays in the schedule, the IC may not be ready to implement DMS. However, DISA and the IC have agreed on the solution to address the directory security requirements; therefore, this report makes no recommendations.

[21] The IC Bypass architecture is composed of legacy switches that provide bi-directional organizational messaging between DMS and legacy users. It is scheduled for closure in September 2004.

Appendix A. Scope and Methodology

We performed this audit to determine whether DMS can replace the critical messaging capabilities of AUTODIN.

To accomplish the audit objective, we:

- visited, contacted, and conducted interviews with officials from OASD(C3I); the Office of the Director, Program Analysis and Evaluation; the Office of the Joint Chiefs of Staff; the Services' DMS Program offices; selected unified commands (the U.S. Pacific Command, the U.S. European Command, the U.S. Transportation Command, and the U.S. Strategic Command); selected subordinate unified commands (U.S. Forces Japan and U.S. Forces Korea); the Air Force Communications Agency; DISA; and the DISA DMS Program Management Office;

- visited, contacted, and conducted interviews with officials from the IC, including the IC Chief Information Officer, the IC DMS Management Office, the Defense Intelligence Communication Accreditation Support Team, the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, the National Imagery and Mapping Agency, and various intelligence field offices; and

- reviewed various reports for the DMS Program that included cost, schedule, and performance parameters covering FY 1990 through FY 2013.

We interviewed officials within OASD(C3I) and the Office of the Joint Chiefs of Staff concerning their respective roles in the oversight of the DMS Program. We interviewed personnel from the DISA DMS Program Management Office, Service DMS program offices (Army, Navy, Air Force, and Marine Corps), and unified command DMS program offices (U.S. Pacific Command, U.S. European Command, U.S. Transportation Command, and U.S. Strategic Command) to determine their respective DMS fielding status. During visits to the unified commands, subordinate unified commands, and DISA, we interviewed personnel responsible for operating DMS to determine whether DMS was fulfilling the users' requirements. We also interviewed officials within DISA to determine the current development and implementation status of DMS.

We reviewed documentation provided by the Services' DMS program offices to evaluate the Services' DMS fielding status and transition plans. We reviewed the DoD Acquisition Regulations (5000 Series) and the OASD(C3I) memorandum, "Policy Guidance for the Defense Message System," February 19, 1998, to determine roles and responsibilities for the DMS Program. In addition, we reviewed "Change 2 to Multicommand Required Operational Capability," October 1, 1997, to determine the specific capabilities required of DMS.

We reviewed and analyzed documentation provided by DISA, including JITC test results (January 2001 and January 2002), the DMS acquisition program baseline (June 2002), life-cycle cost estimate (July 2002), analysis of alternatives (June 14, 2002), DMS business process reengineering assessment (June 14, 2002), and benefits analysis (June 24, 2002). We also reviewed documentation provided by the IC, such as “Intelligence Community (IC) Requirements & Analysis Report,” July 15, 1998, and “DMS Release 3.0 IC Priority 1 Requirements Implementation Matrix,” January 7, 2000, provided by the IC, which lists the most critical requirements of the IC. We reviewed documentation from each IC agency to determine whether a stable DMS architecture was in place. We analyzed documentation provided by DISA and the IC regarding the development of the DMS directory, including the OASD(C3I) memorandum, “DMS Directory Security Requirements,” June 26, 2002, and the FCD.

We performed this audit from April 2002 through March 2003 in accordance with generally accepted government auditing standards. Our scope was limited in that we did not include tests of management controls.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of the DoD Systems Modernization high-risk area.

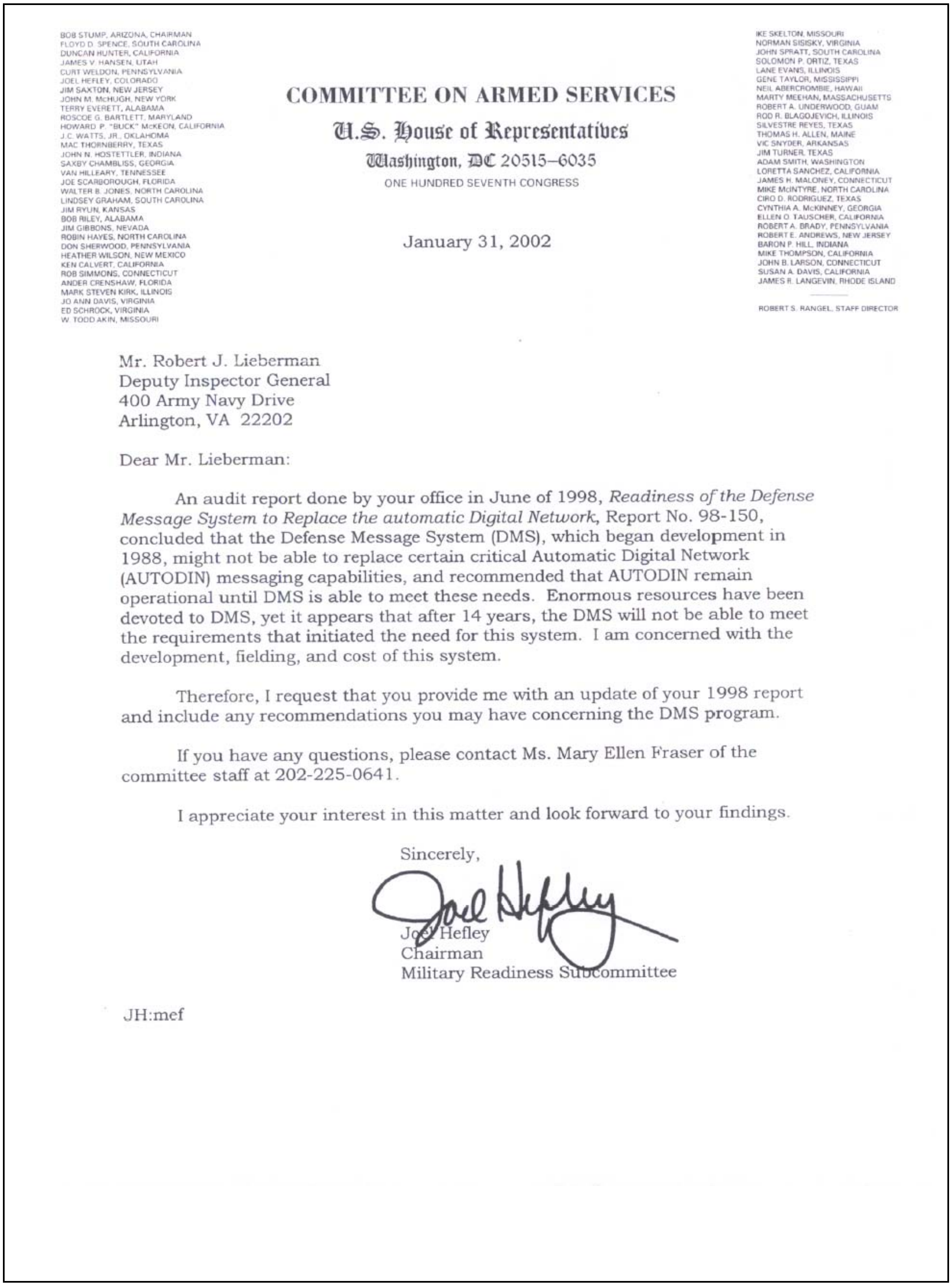
Prior Coverage

During the last 5 years, the Inspector General of the Department of Defense (IG DoD) has issued one report discussing the transition from AUTODIN to DMS. Unrestricted IG DoD reports can be accessed at http://www.dodig.osd.mil/audit/reports.

IG DoD

IG DoD Report No. 98-150, “Readiness of the Defense Message System to Replace the Automatic Digital Network,” June 11, 1998

Appendix B. Congressional Request



COMMITTEE ON ARMED SERVICES
U.S. House of Representatives
Washington, DC 20515–6035
ONE HUNDRED SEVENTH CONGRESS

January 31, 2002

Mr. Robert J. Lieberman
Deputy Inspector General
400 Army Navy Drive
Arlington, VA 22202

Dear Mr. Lieberman:

An audit report done by your office in June of 1998, *Readiness of the Defense Message System to Replace the automatic Digital Network*, Report No. 98-150, concluded that the Defense Message System (DMS), which began development in 1988, might not be able to replace certain critical Automatic Digital Network (AUTODIN) messaging capabilities, and recommended that AUTODIN remain operational until DMS is able to meet these needs. Enormous resources have been devoted to DMS, yet it appears that after 14 years, the DMS will not be able to meet the requirements that initiated the need for this system. I am concerned with the development, fielding, and cost of this system.

Therefore, I request that you provide me with an update of your 1998 report and include any recommendations you may have concerning the DMS program.

If you have any questions, please contact Ms. Mary Ellen Fraser of the committee staff at 202-225-0641.

I appreciate your interest in this matter and look forward to your findings.

Sincerely,

Joel Hefley

Joel Hefley
Chairman
Military Readiness Subcommittee

JH:mef

Appendix C. DMS Multicommand Required Operational Capability Requirements

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.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
  Director, Program Analysis and Evaluation
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Director, Defense Procurement and Acquisition Policy

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Unified Commands

Commander, U.S. Northern Command
Commander, U.S. Southern Command
Commander, U.S. Joint Forces Command
Commander, U.S. Pacific Command
  Commander, U.S. Forces Japan
  Commander, U.S. Forces Korea
Commander, U.S. European Command
Commander, U.S. Central Command
Commander, U.S. Transportation Command
Commander, U.S. Special Operations Command
Commander, U.S. Strategic Command

Other Defense Organizations

Director, Defense Information Systems Agency
Director, Defense Intelligence Agency
Director, National Imagery and Mapping Agency
Director, National Reconnaissance Office
Director, National Security Agency

Non-Defense Federal Organizations

Office of Management and Budget
Director, Central Intelligence Agency

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Subcommittee on Military Readiness, Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Team Members

The Readiness and Logistics Support Directorate, Office of the Assistant Inspector General for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Shelton R. Young
Kimberley A. Caprio
Donald A. Bloomer
Lieutenant Colonel Shannon Jones, U.S. Army
Vanessa Springfield
Suk Y. Webb
Keith M. Owens
Velma E. White
Gary L. Queen
Michael J. Roark
Deirdre Beal
April L. Glasscock
Joshua H. Hickman
Robert E. L. Smith
Mandie L. Marr
Elizabeth N. Shifflett