Audit Report

READINESS OF THE DEFENSE MESSAGE SYSTEM TO REPLACE THE AUTOMATIC DIGITAL NETWORK

Report No. 98-150 June 11, 1998

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 or visit the Inspector General, DoD, Home Page at: WWW.DODIG.OSD.MIL

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: APTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

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, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASC	AUTODIN Switching Center
ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
AUTODIN	Automatic Digital Network
DISA	Defense Information Systems Agency
DMS	Defense Message System
MAIS	Major Automated Information System
MAISRC	Major Automated Information Systems Review Council
MROC	Multi-Command Required Operational Capabilities
ROMC	Required Operational Messaging Characteristics

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

June 11, 1998

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

SUBJECT: Audit Report on the Readiness of the Defense Message System to Replace the Automatic Digital Network (Report No. 98-150)

We are providing this report for information and use. We considered management comments on a draft of this report in preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are necessary.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Harlan M. Geyer at (703) 604-9594 (DSN 664-9594) or at e-mail address hgeyer@dodig.osd.mil, or Mr. Ralph S. Dorris at (703) 604-9584 (DSN 664-9584) or at e-mail address rdorris@dodig.osd.mil. See Appendix E for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 98-150 **June 11, 1998**
(Project No. 7RA-0049)

Readiness of the Defense Message System to Replace the Automatic Digital Network

Executive Summary

Introduction. The Automatic Digital Network (AUTODIN) has provided DoD messaging capability since 1962. However, the system uses antiquated technology and is very expensive to operate and maintain. The Defense Information Systems Agency began developing the Defense Message System (DMS) in 1988 to replace messaging functions provided by AUTODIN and electronic mail systems.

Audit Objectives. The overall audit objective was to determine the readiness of DMS to replace AUTODIN. Specifically, we intended to determine whether technical issues involved with fielding DMS can be resolved prior to December 1999, the scheduled date to complete the phaseout of AUTODIN, and we intended to determine the effects on messaging capabilities after that date if AUTODIN has year 2000 problems. We also reviewed the adequacy of the management control program related to the overall audit objective.

Audit Results. DMS may not be available to replace some critical AUTODIN messaging capabilities such as classified message processing and emergency action message transmission by December 31, 1999, when the AUTODIN contract expires. Without DMS, critical messaging services will need to be provided by AUTODIN or the mission of the warfighter will be severely impacted. This possible lack of critical messaging capability is due, at least in part, to unanticipated changes in requirements and technical challenges that have occurred since the inception of DMS. We determined that AUTODIN is year 2000 compliant, but some message handling systems that receive messages through AUTODIN are not. Those systems will need to be modified to be year 2000 compliant if they are needed beyond 1999. See Part I for details. The management controls we reviewed were effective in that no material management control weakness was identified. See Appendix A for details of the review of the management control program. See Appendix C for a discussion on DMS program status reporting.

Summary of Recommendations. We recommend that AUTODIN remain operational until DMS is provided. We also recommend that any systems that need to remain connected to AUTODIN beyond December 31, 1999, be upgraded to meet year 2000 compliance. Additionally, any "work-around" systems being developed to replace AUTODIN capabilities should be evaluated to determine continued need if AUTODIN is not phased out as planned.

Management Comments. The Director, Communications, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the finding and recommendations. The Director stated that the

Department will maintain DMS transition hubs with AUTODIN-like switching and translation services to support selected critical systems, allied and coalition, and tactical customers as long as necessary. The Director also stated that all systems connected to transition hubs and those that transition to DMS must be certified year 2000 compliant. Further, all legacy systems that have dependency on AUTODIN are undergoing in-depth review to determine the best support or transition for each system. See Part III for the complete text of comments.

Table of Contents

Executive Summary i

Part I - Audit Results

Audit Background 2
Audit Objectives 3
DoD Messaging Services Beyond December 1999 4

Part II - Additional Information

Appendix A. Audit Process
Scope and Methodology 12
Management Control Program 13
Appendix B. Summary of Prior Coverage 14
Appendix C. Defense Message System Status Reporting 17
Appendix D. Multi-Command Required Operational Capabilities Requirements 19
Appendix E. Report Distribution 20

Part III - Management Comments

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments 24

Part I - Audit Results

Audit Background

Electronic Mail. The use of electronic mail (e-mail) increased significantly in the 1980s as technology advanced, making it an effective means of exchanging information. E-mail systems had been fielded that were unique to individual manufacturers. Those unique systems adversely affected the transmission of information between networks because manufacturers did not use the same standard in developing e-mail systems. Although procedures were developed to allow the reader to understand messages transferred from one e-mail system to another, those procedures did not provide the full range of functions needed for an effective messaging system.

Defense Message System. The Defense Information Systems Agency (DISA) began developing the Defense Message System (DMS) in 1988 to provide a global e-mail system. DMS resulted from an initiative by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD[C^3I]) to determine future DoD electronic messaging systems. The key factors that led to this effort were the imposition of severe budgetary constraints, the obsolescence of existing systems, and the emergence of new messaging standards and technology. A DoD consensus was reached to modernize DoD messaging services through an evolutionary process. As a part of this process, DISA, along with the Military Departments, established DMS program offices to develop messaging systems, architectures, and transition plans. DISA and the Military Departments agreed that DISA would provide all software products and that the cost of fielding the hardware products would be shared. Those plans have evolved through several iterations of improvement and maturity.

DMS will result in the implementation of a global e-mail system using commercial off-the-shelf products to conduct secure business-grade messaging throughout DoD. DMS consists of the collection of all DoD messaging hardware, software, communications facilities, procedures, and personnel organized into a system that will serve as a single, seamless system supporting administrative, command and control, intelligence, and other base functions. DMS will incorporate evolving technologies to provide a secure e-mail system, capable of handling all message traffic, and a directory of all users. Message writers will be able to use DMS to always reach their intended readers worldwide, and be assured the message is secure. As of February 1998, $226 million had been obligated to develop DMS.

System Responsibilities. ASD(C^3I) is responsible for providing programmatic, policy and acquisition guidance, and oversight for DMS. DISA is responsible for providing overall operational management and control of DMS, to include ensuring that Joint Staff requirements are met, coordinating the implementation of DMS DoD-wide, performing compliance test and evaluation of components, and providing system administrators with initial and follow-on training to ensure operational capability. DMS will replace existing e-mail systems and the Automatic Digital Network (AUTODIN).

Automatic Digital Network. AUTODIN, a messaging system that DoD has used since 1962 to exchange messages electronically among organizations, allows users to securely transmit messages ranging from unclassified to top secret, including sensitive compartmented information. The message traffic travels through AUTODIN Switching Centers (ASCs) to DoD agencies, the Services, and U.S. and allied forces throughout the world. As of February 1998, there were eight ASCs remaining. Two ASCs are scheduled to close by December 1998 and a third is scheduled to close in April 1999. The remaining five ASCs, located at Fort Detrick, Maryland; Hancock, New York; McClellan Air Force Base, California; Pirmasens, Germany; and Wahiawa, Hawaii, are scheduled to close in December 1999. Before those last five ASCs can be closed, certain DMS technologies must be in place.

Audit Objectives

The overall audit objective was to determine the readiness of DMS to replace AUTODIN. Specifically, we intended to determine whether technical issues involved with fielding DMS could be resolved prior to December 1999, the scheduled date to complete the phaseout of AUTODIN, and we intended to determine the effects on messaging capabilities after that date if AUTODIN has year 2000 problems. We also reviewed the adequacy of the management control program as it applied to the overall audit objective. See Appendix A for a discussion of the audit scope and methodology and for the results of the review of the management control program. See Appendix B for a summary of prior coverage related to the objectives. See Appendix C for a discussion on DMS program status reporting.

DoD Messaging Services Beyond December 1999

DMS may not be available to replace some critical AUTODIN messaging capabilities by December 31, 1999, when the AUTODIN contract expires. Changes in requirements and technical challenges not initially anticipated caused delays in the development and fielding of DMS. If DMS is not available by December 31, 1999, critical messaging services will need to be provided by AUTODIN or the mission of the warfighter could be severely impacted.

AUTODIN

Since 1962, AUTODIN has been the primary means for DoD to satisfy requirements for message communications. Although the system has been modernized and undergone numerous enhancements over its 35-year life span, it is still based on an architecture developed in the late 1950s and is considered to be manpower intensive by today's standards. In January 1988, ASD(C^3I) formed a working group to consider a replacement for AUTODIN.

According to the DISA contracting office, the AUTODIN contract was a sole-source award to Contel Federal Systems, a subsidiary of GTE Service Corporation. The AUTODIN contract with GTE will expire on December 31, 1999. If AUTODIN service is needed beyond December 31, 1999, DISA will need to award a new sole-source contract to GTE.

DMS

ASD(C^3I) formed the Multi-Service and Agency Defense Message System Working Group in January 1988 to assess the future of DoD messaging systems. ASD(C^3I) approved DMS and the transition approach in May 1988, and the Under Secretary of Defense for Acquisition issued DMS program guidance in August 1988. In February 1989, the Joint Chiefs of Staff approved the Multi-Command Required Operational Capabilities (MROC), which were subsequently updated in October 1990, April 1993, and August 1997. See Appendix D for a list of the 13 required capabilities in the MROC.

Year 2000

The year 2000 represents a unique challenge for systems, such as a message handling system, that are date dependent. Information technology systems have typically used two digits to represent the year, such as "97" to represent 1997, to conserve electronic data storage and reduce operating costs. With the

two-digit format, the year 2000 would be represented as "00," making it indistinguishable from the year 1900. As a result of this ambiguity, computers and associated systems and application programs that use dates to calculate, compare, and sort information, could generate incorrect results when working with years after 1999. The Chief Information Officer, DoD, is managing DoD efforts to address the year 2000 computing challenge.

DMS is being developed to be year 2000 compliant. If DMS is not able to meet critical messaging requirements by December 1999 and AUTODIN is extended into the year 2000, all systems that will use AUTODIN must be year 2000 compliant.

DMS Availability

DMS may not be available to replace some critical AUTODIN messaging capabilities by December 31, 1999, when the AUTODIN contract expires. Initial operational capability is scheduled to be available prior to January 1, 2000, and full operational capability is scheduled for sometime in the year 2008. However, that schedule was based on DMS-compliant components being available for deployment in 1996. Many of those components were not approved for deployment until 1997. We attribute the non-availability of critical messaging capabilities to unanticipated changes in requirements and technical challenges, resulting in system development and fielding delays.

DMS Requirements Changes. From its inception, DMS experienced changes in its requirements, which impacted the timely development and fielding of the system. Initial contract award was also delayed. Although the development of DMS was approved in May 1988, the DMS contract was not awarded until May 1995. Due to a protest of the contract award, work under the contract was delayed until August 1995.

DMS Requirements. Changes in requirements impacted DMS development. The DMS requirements baseline is a combination of the MROC and the Required Operational Messaging Characteristics (ROMC). In April 1994, the Joint Chiefs approved the DMS ROMC developed by DISA. The DMS ROMC provided 94 more specific, detailed, and, where possible, quantitative and qualitative statements of requirements listed in the DMS MROC. Although refining requirements helps ensure that the fielded system meets user needs, it can affect timely system development. For example, the need to process classified intelligence messages was not an original DMS requirement, but it was identified as a requirement in 1994. Although the effect cannot be quantified, DISA and the intelligence community acknowledge that DMS intelligence message processing will not be available by December 31, 1999. Conversely, the 1997 DMS requirements review should improve the timeliness of system development.

DMS Requirements Review. From February through June 1997, Service communications principals reviewed and revalidated the requirements baseline. The primary purpose of this examination was to update DMS requirements as stated in the MROC and the ROMC to ensure DMS would meet the fiscal, operational, and technological realities of today and the future. The Service communications principals also wanted to ensure that DMS was based on commercial off-the-shelf products to the maximum extent possible. The Service communications principals revalidated the intent of the original 13 MROC requirements. However, 50 of the 94 (53 percent) DMS ROMC requirements were not revalidated during this review. Of those 50 requirements, 20 were deleted, 21 were merged or moved outside the DMS ROMC, and 9 were considered redundant. The remaining revalidated MROC and ROMC requirements reduced DoD messaging requirements, ensured more commercial off-the-shelf products could be used for DMS, and reduced the costs for fielding DMS. Although the exact amount of time could not be determined, the DMS requirements review reduced system development time because the principals made a decision not to revalidate 53 percent of the ROMC requirements. As a result of the review, the DMS MROC and the ROMC were combined into one document: "Change 2 to DMS MROC 3-88," October 30, 1997.

DMS Technical Challenges. DMS technology has not advanced as initially envisioned. When DMS was approved in 1988 and when the phase-in plan was written in 1996, the development was based on the assumption that several technical issues and critical messaging capabilities would be resolved before the AUTODIN phaseout. In order to develop the AUTODIN phaseout plan, the DMS Working Group made several assumptions.

- DMS would be capable of satisfying the unclassified through top secret messaging requirements currently satisfied by AUTODIN.

- The multifunctional interpreter, a transitional component, would provide interoperability between AUTODIN and DMS for those entities not transitioning immediately and between systems used by non-DoD agencies (to include U.S. allies) and DMS.

- The DMS infrastructure would be in place by December 31, 1999, to support base, post, camp, station, or organization transition from AUTODIN.

Those technical issues and critical messaging capabilities must be resolved before the transition from AUTODIN to DMS can be completed. As of May 1998, they had not been resolved.

With the delay in technological development of DMS, system testing has been delayed. The initial operational test and evaluation was scheduled for January 1996, but was not completed until August 1997. Any additional slippage could delay initial operational capability and critical messaging capabilities.

Critical Messaging Capabilities. Any delay in fielding DMS will impact critical messaging capabilities and year 2000 compliance.

Classified Message Processing. DoD organizations' and U.S. allies' capability to transmit and receive classified messages could be interrupted after December 1999 if AUTODIN is phased out by that date and DMS technology is not available for classified message transmission. National security could be affected if classified messages were not delivered on secure lines in a timely manner. Therefore, a minimum number of AUTODIN circuits and switching centers should remain open to support classified message transmission requirements.

Emergency Action Message Requirements. DMS is not yet capable of meeting emergency action message transmission requirements. Three main requirements exist for transmitting emergency action messages: speed of delivery, guarantee of delivery, and ability to send messages at different levels of classification. A fourth requirement is the ability to send messages to 100 addressees worldwide. Although speed of delivery is a Military Department and Defense agency responsibility, not a DMS requirement, the communications infrastructure would have to accommodate the emergency action message transmission requirement.

Year 2000 Compliance. Year 2000 compliance of DoD messaging systems would be impacted by a delay in fielding DMS and reliance on AUTODIN. The Army has three AUTODIN message handling systems that are not year 2000 compliant. Those message handling systems transmit data on AUTODIN. If those AUTODIN message handling systems are not made year 2000 compliant, critical messaging services will not be available to the Army. Fixes had been proposed but were expensive, so the Army planned not to fix the systems because they were scheduled to be replaced by DMS.

Continued Capability

With the possible delay in fielding DMS, critical messaging services beyond 1999 may need to be provided through the continuation of the AUTODIN contract. That will severely impact the mission of DoD communications centers, which will have to support both AUTODIN and DMS messages, but which do not have the funding or manpower to provide that support.

AUTODIN Continuation. AUTODIN can continue to provide critical messaging capabilities beyond 1999. AUTODIN is year 2000 compliant, but some message handling systems, and possibly other data processing systems, that receive messages through AUTODIN are not year 2000 compliant. If these systems are needed beyond 1999, they need to be modified to be year 2000 compliant.

New Contract Award. The 10-year telecommunications contract for AUTODIN expires on December 31, 1999. If AUTODIN needs to be extended beyond 1999, the only option for DISA is to award a new, sole-source contract to GTE. No other contractor has the ability to provide AUTODIN services without an expenditure of enormous cost and time.

AUTODIN-Like Systems. The Services were developing "work-around" systems to reduce and eventually eliminate connections to AUTODIN, based on the AUTODIN closure date of December 31, 1999. Those systems would duplicate capabilities that existed with AUTODIN. For example, the Air Force was developing an Interim Record Communications Architecture. The Interim Record Communications Architecture would allow several bases in a region to connect to one Air Force base and send message traffic to an ASC on one circuit, instead of using an individual circuit for each base. As DMS is implemented over the next two years, all Air Force systems that DMS can support will switch to DMS. The Interim Record Communications Architecture would continue supporting message traffic for some Air Force remote sites until DMS is fielded at those sites at a later date.

The continued development of each work-around system should be evaluated if AUTODIN were to be retained beyond December 31, 1999. However, if those systems are being developed in response to the ASD(C^3I) transitional messaging initiative, those systems must demonstrate year 2000 compliance. The ASD(C^3I) transitional messaging initiative directed that all computer-to-computer messages (such as the transmission of large amounts of equipment usage or repair data), known as data pattern traffic, be removed from AUTODIN.

Summary

Although DMS should provide advanced technological capabilities once implemented, it still has technical challenges and additional messaging requirements that may not be resolved by December 1999. A decision needs to be made to develop contingency plans that ensure continued messaging capabilities for all users in case DMS issues are not resolved by December 1999.

Recommendations, Management Comments, and Audit Response

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

1. Keep the Automatic Digital Network operational, if required, until the Defense Message System is provided to DoD users and U.S. allies.

2. Take action to ensure that all systems that remain connected to the Automatic Digital Network beyond December 1999 are year 2000 compliant.

3. Require all users to evaluate the continued need to develop work-around systems if the Automatic Digital Network is not phased out as planned, unless the work-around systems are transitional messaging initiatives developed in response to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) mandate concerning data pattern traffic.

Management Comments. The Director, Communications, Office of the Assistant Secretary of Defense, (Command, Control, Communications, and Intelligence) concurred. The Director stated that the Department would maintain DMS transition hubs with AUTODIN-like switching and translation services to support selected critical systems, allied and coalition, and tactical customers as long as necessary. The Director also stated that all systems connected to transition hubs and those that transition to DMS must be certified year 2000 compliant, and that all legacy systems that have dependency on AUTODIN are undergoing in-depth review to determine the best support or transition for each system.

Part II - Additional Information

Appendix A. Audit Process

Scope and Methodology

Scope and Methodology. We reviewed the "DoD Master Plan for the Phase-out of AUTODIN," March 14, 1997, and an associated "DMS Phase-In Supplement," June 30, 1997. Those plans listed critical DMS capabilities that must be in place before the last ASCs are closed. We reviewed the DMS requirements documents (MROC and ROMC) to determine the system baseline and changes thereto. We reviewed the current status of the DMS program to determine whether those critical DMS capabilities could be attained by December 31, 1999. We also reviewed cost data from the DMS contract. We examined "DMS Prologue to the Government E-Mail Revolution," June 19, 1995, for a definition, key milestone dates, and benefits of DMS. We interviewed personnel at the DISA DMS Program Office and at Army, Navy, and Air Force DMS program offices. We also interviewed personnel from the office of the ASD(C^3I), the Joint Staff, the U.S. Pacific Command, and the U.S. Space Command. In addition, we interviewed the AUTODIN contracting officer to obtain information on the contract status. We reviewed the draft Initial Operational Test and Evaluation report for DMS Version 1.0, September 1997, and the 1997 DMS quarterly Major Automated Information System (MAIS) status reports. See Appendix C for a discussion of DMS program status reporting.

DoD-wide Corporate Level Government Performance and Results Act (GPRA) Goals. In response to the GPRA, the Department of Defense has established 6 DoD-wide corporate level performance objectives and 14 goals for meeting those objectives. This report pertains to achievement of the following objectives and goals.

- **Objective:** Maintain highly ready joint forces to perform the full spectrum of military activities. **Goal:** Maintain high military personnel and unit readiness. **(DoD-5.1)**

- **Objective:** Fundamentally reengineer DoD and achieve a 21st century infrastructure. **Goal:** Reduce costs while maintaining required military capabilities across all DoD mission areas. **(DoD-6)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following information technology management functional area objectives and goals.

- **Objective:** Provide services to satisfy customer information needs. **Goal:** Modernize and integrate Defense information infrastructure. **(ITM-2.2)**

Appendix A. Audit Process

Scope and Methodology

Scope and Methodology. We reviewed the "DoD Master Plan for the Phase-out of AUTODIN," March 14, 1997, and an associated "DMS Phase-In Supplement," June 30, 1997. Those plans listed critical DMS capabilities that must be in place before the last ASCs are closed. We reviewed the DMS requirements documents (MROC and ROMC) to determine the system baseline and changes thereto. We reviewed the current status of the DMS program to determine whether those critical DMS capabilities could be attained by December 31, 1999. We also reviewed cost data from the DMS contract. We examined "DMS Prologue to the Government E-Mail Revolution," June 19, 1995, for a definition, key milestone dates, and benefits of DMS. We interviewed personnel at the DISA DMS Program Office and at Army, Navy, and Air Force DMS program offices. We also interviewed personnel from the office of the ASD(C^3I), the Joint Staff, the U.S. Pacific Command, and the U.S. Space Command. In addition, we interviewed the AUTODIN contracting officer to obtain information on the contract status. We reviewed the draft Initial Operational Test and Evaluation report for DMS Version 1.0, September 1997, and the 1997 DMS quarterly Major Automated Information System (MAIS) status reports. See Appendix C for a discussion of DMS program status reporting.

DoD-wide Corporate Level Government Performance and Results Act (GPRA) Goals. In response to the GPRA, the Department of Defense has established 6 DoD-wide corporate level performance objectives and 14 goals for meeting those objectives. This report pertains to achievement of the following objectives and goals.

- **Objective:** Maintain highly ready joint forces to perform the full spectrum of military activities. **Goal:** Maintain high military personnel and unit readiness. **(DoD-5.1)**

- **Objective:** Fundamentally reengineer DoD and achieve a 21st century infrastructure. **Goal:** Reduce costs while maintaining required military capabilities across all DoD mission areas. **(DoD-6)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following information technology management functional area objectives and goals.

- **Objective:** Provide services to satisfy customer information needs. **Goal:** Modernize and integrate Defense information infrastructure. **(ITM-2.2)**

- **Objective:** Ensure that DoD vital information resources are secure and protected.
  Goal: Build information assurance architecture and supporting services. **(ITM-4.2)**

General Accounting Office High Risk Area. The General Accounting Office (GAO) has identified several high risk areas in DoD. This report provides coverage of the Information Management and Technology high risk area.

Audit Type, Dates, and Standards. We performed this program audit from June 1997 through May 1998, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. Accordingly, we included tests of management controls considered necessary. No computer-processed data were used in the course of this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within the DoD. Further details are available on request.

Management Control Program

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of Review of Management Control Program. We reviewed the adequacy of DISA management controls over the DMS program. Specifically, we reviewed the DMS Program Office management control procedures over the implementation of DMS. Because we did not identify a material weakness, we did not assess management's self-evaluation.

Adequacy of Management Controls. The DISA DMS Program Office management controls over the DMS program implementation were adequate as they applied to the audit objectives.

Appendix B. Summary of Prior Coverage

In the past 5 years the Inspector General, DoD, has issued four reports dealing with the DMS and related issues.

Inspector General, DoD, Report No. PO 97-024, "Management of Multilevel Security Applications for DoD Systems," June 12, 1997, states that the security for automated information systems are insufficient and that standards for sensitivity labeling of automated information systems data storage had not been developed. The report recommended that ASD(C^3I) establish security policies and procedures unique to automated information systems; develop a sensitivity labeling standard for automated information systems data storage and processing; and establish policy to implement the standard throughout DoD. The report also recommended that policies and procedures be established to require coordination of all DoD multilevel security initiatives with the DoD Multilevel Security Program Office and that the DoD Multilevel Security Program Office be provided adequate authority and resources to coordinate DoD multilevel security initiatives.

ASD(C^3I) replied that a new directive for security for automated information systems would be available October 1997; that a Secret and Below Interoperability Memorandum requiring the use of the DoD Security Certification and Accreditation Process for Information Technology was signed March 1997; that a labeling policy was being coordinated and should be released soon; and that initiatives were in place to provide coordination and oversight of the management of multilevel security initiatives. ASD(C^3I) also replied that the DoD Multilevel Security Program Office needed an appropriate level of resources to accomplish its responsibilities. In the final report, ASD(C^3I) was requested to provide dates for documents not published and a plan of action for obtaining resources needed by the Multilevel Security Program Office. Management responded positively by providing the publication dates for the publications and a draft plan of action to obtain needed multilevel security resources.

Inspector General, DoD, Report No. 97-031, "Phase out of the Automatic Digital Network," November 25, 1996, states that planning for Command Communications Service Designators and circuit lists for military plans were incomplete and that not all circuits that had been moved had been connected to another ASC. The report recommended that all plans show the Command Communications Service Designators for all the circuits at each switching center; that circuits moved from one ASC to another be reconnected to one of the last four remaining ASCs; and that circuits listed in Military Department plans be reconciled to the universe of the AUTODIN circuits reflected in the DoD Master Plan. The Director, DISA, concurred with two of the recommendations and partially concurred with the third recommendation. The Director, DISA, stated that a circuit not reconnected to one of the remaining ASCs would transition to DMS before the closure of the ASC to which the circuit was reconnected. Management comments were responsive to the recommendations.

Inspector General, DoD, Report No. 95-269, "Oversight Process of the Major Automated Information Systems Review Council," June 30, 1995, states that procedural guidance was insufficient in the area of management information systems processes. The report recommended revising DoD regulations to specify procedures that will involve the MAISRC in ongoing DoD Corporate Information Management Initiative efforts and to specify procedures for the MAISRC to use in performing independent assessments of the selection and development of MAISs that will be used on a DoD-wide basis. The report also recommended revising guidance to specify procedures for performing operational testing and for validating costs and benefits of automated information systems developed in increments; determining key, minimum documentation for each type of MAISRC review; and clarifying oversight responsibility for command, control, communications, and intelligence MAISs.

The Deputy Assistant Secretary of Defense (Acquisition) concurred with most of the recommendations. Management would consider clarifying procedures for the oversight of incrementally developed systems. Management did not agree that procedures should be specified to involve the MAISRC staff in Corporate Information Management Initiative efforts, including the selection and development of migratory systems. As a result of management comments, recommendations concerning the oversight of incrementally developed systems and enhanced cost and benefit validations were revised to clarify intent. Management comments to the revised recommendations were responsive.

Inspector General, DoD, Report No. 95-084, "Hotline Allegations Concerning a Request for Proposal for the Defense Message System," January 26, 1995. The report discussed the validity of allegations made to the Defense Hotline related to the request for proposal for DMS. Specifically, the allegations related to three categories: the cost of DMS was understated, the required multilevel security environment was not defined, and the future requirements were not identified in the request for proposal. Allegations concerning the multilevel security environment and future requirements for DMS could not be substantiated. The allegation that the cost of DMS was understated had merit.

The report recommended that approval to award the DMS contract be delayed until the MAISRC reviewed and validated program cost data for completeness and accuracy; that a Milestone III review for the DMS program be conducted; that funding be withheld from DMS until program costs and cost-benefit analyses were reviewed and validated; that DMS cost data be corrected to reflect that the cost of the Government-furnished microchip and the costs to upgrade the baseline system could be an alternative to the baseline system; and that controls be established to recover the cost of the microchip when DMS equipment is sold to non-DoD agencies.

Management planned to award the contract, but agreed to limit funding obligations to $55 million while cost estimates were validated. The MAISRC reviewed the proposed contract award for DMS and provided the System Decision Memorandum, which established requirements for the Milestone III review. Management agreed to include the cost of the Government-furnished

microchip in the DMS cost, but did not agree to show the costs to upgrade the baseline system as an alternative to the baseline system. Management established controls to ensure cost recovery of the microchip.

Appendix C. Defense Message System Status Reporting

Status reports on the DMS program did not identify some program issues, problems, and risks. Additionally, overall assessments of major program areas did not accurately assess the status of the DMS program.

Program Oversight. The DMS program had been designated as a MAIS, which is subject to oversight by the MAISRC. The MAISRC is the DoD senior level forum for advising ASD(C^3I) on critical decisions concerning the acquisition of designated MAISs. The MAISRC is chaired by ASD(C^3I) and includes representatives from the Under Secretary of Defense for Acquisition and Technology; the Under Secretary of Defense (Comptroller); the Director of Operational Test and Evaluation; the Director of Program Analysis and Evaluation; the Director, Joint Staff; and user representatives.

Oversight Requirements. DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," March 15, 1996, establishes a periodic reporting system for MAISs. DoD 5000.2-R, Part 6, states that:

> The quarterly MAIS status reporting system is designed to provide executive management at the Office of the Secretary of Defense and component levels with the program status, progress, issues, risks, and risk reducers. The quarterly report is essential to the early identification of problems and associated plans to initiate corrective actions.

According to DoD 5000.2-R, the DISA DMS Program Office is required to provide a quarterly MAIS status report to the MAISRC. The program manager's assessment of the DMS program should be included in the quarterly MAIS status report.

Quarterly Status Reports. The quarterly MAIS status reports for DMS rarely identified DMS program issues, problems, and risks. The FY 1997 reports did not provide any meaningful information on key program problem areas such as multilevel security message processing, multifunctional interpreters, emergency action message requirements, and continued schedule delays.

Program Assessments. Overall assessments of major programmatic areas did not accurately assess the status of the DMS program. The DMS quarterly MAIS status reports included a program manager's assessment of 10 major programmatic areas: program cost, approved funding, schedule, requirements, technical risks, contracts, staffing, test and evaluation, training,

and security. The program manager provided a summary assessment of the status of each major programmatic area using the codes green (satisfactory), yellow (marginal), and red (unsatisfactory). In the report for fourth quarter, 1997, all 10 major programmatic areas were assessed as satisfactory. At a minimum, we believe the schedule should be assessed as marginal given major schedule delays to date. We also believe that a number of technical challenges and risks involved in developing multilevel security and multifunctional interpreter solutions should have been included in the DMS quarterly MAIS status reports.

Although there are other means of advising senior management of DMS program status, progress, and issues, the DMS quarterly MAIS status report was designated as the formal method for early identification of DMS problems and plans for corrective action. If this report does not accurately assess and discuss programmatic issues, the quarterly assessments may not convey the true status of the DMS program.

Appendix D. Multi-Command Required Operational Capabilities Requirements

The 13 MROC requirements for the DMS are:

1. Timely Delivery
2. Identification of Recipients
3. Integrity
4. Availability/Reliability
5. Guaranteed Delivery/Accountability
6. Confidentiality/Security
7. Storage and Retrieval Support
8. Connectivity/Interoperability
9. Ease of Use
10. Message Preparation Support
11. Distribution Determination and Delivery
12. Authentication
13. Survivability

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

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

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
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 in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
  Office of Information and Regulatory Affairs
Technical Information Center, National Security and International Affairs Division, General Accounting Office

Chairman and ranking minority member of each of the following congressional committees and subcommittees:

  Senate Committee on Appropriations
  Senate Subcommittee on Defense, Committee on Appropriations
  Senate Committee on Armed Services
  Senate Committee on Governmental Affairs
  Senate Select Committee on Intelligence
  House Committee on Appropriations
  House Subcommittee on National Security, Committee on Appropriations
  House Committee on Government Reform and Oversight
  House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight
  House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform and Oversight
  House Committee on National Security

Part III - Management Comments

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

20 May 1998

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING (OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE)

SUBJECT: DoDIG Draft Audit Report, Readiness of Defense Message System (DMS) to Replace AUTODIN, (**Project N. 7RA-0094**)

We concur with the finding that DMS may not be able to support some critical systems currently dependent upon AUTODIN by December 31, 1999.

Recommendation 1. Keep the AUTODIN operational, if required, until the DMS is provided to DoD users and U.S. allies. The Department will maintain DMS Transition Hubs with AUTODIN-like switching and translation services to support selected critical systems, allied/coalition, and tactical customers as long as necessary.

Recommendation 2. Take action to ensure that all systems that remain connected to the AUTODIN beyond December 1999 are year 2000 (Y2K) compliant. All systems within DoD must be certified Y2K compliant to include those systems connected to the transition hubs and those that transition to DMS.

Recommendation 3. Require all users to evaluate the continued need to develop work-around systems if the AUTODIN is not phased out as planned, unless the work-around systems are transitional messaging initiatives developed in response to the ASD/C3I mandate concerning data pattern traffic. All legacy systems that have a dependency on AUTODIN are undergoing in-depth review by the Department Chief Information Officers (CIO). These reviews will determine the best support or transition for each system and reported to DoD CIO in July, with periodic updates as necessary.

The point of contat in the office of the Director, Communications is Ms. Oma Elliott. She can be reached at (703) 697-7627, or oma.elliott@osd.pentagon.mil.

Richard M. Dyson
Director, Communications

Audit Team Members

This report was prepared by the Readiness and Logistics Support Directorate, Office of the Assistant Inspector General for Auditing, DoD.

Shelton R. Young
Harlan M. Geyer
Ralph S. Dorris
Lorin T. Pfeil
Dennis R. Wade
Sheree A. Thompson
John D. McAulay