

DEFENSE MESSAGE SYSTEM (DMS)



DISA ACAT IAM Program

Total Number of Systems:	7000+ sites
Total Program Cost (TY\$):	\$1.6B
Life-Cycle Cost (TY\$):	\$5B
Full-rate production:	2QFY98

Prime Contractor

Lockheed Martin Federal Systems

SYSTEM DESCRIPTION & CONTRIBUTION TO JOINT VISION 2010

The Defense Message System (DMS) contributes to the *information superiority* necessary to achieve *Joint Vision 2010* by enabling anyone in DoD to exchange messages with anyone else in DoD. This is accomplished by a worldwide, secure, accountable, and reliable, reader-to-writer messaging system. DMS, with associated bridging systems, is to replace the official “organizational” messaging system—the Automatic Digital Network (AUTODIN). This is intended to reduce the cost and manpower demands of the legacy system based on 1960s technology. To accomplish this, DMS must be implemented on over 360,000 desktop computers at over 7,000 sites worldwide and support message exchanges with tactical forces, allies, other designated federal government users, and defense contractors. DMS must also provide ordinary E-mail (“individual” messaging) by handling both commercial and classified messages. The DMS program capitalizes on existing and emerging commercial messaging technology by employing the international X.400 messaging standard and X.500 directory services standard. DMS is a value-added service operating on the programmatically separate Defense Information Infrastructure computer and communications backbone. The National Security Agency has taken

responsibility for DMS security services based on the Multi-level Information System Security Initiative (MISSI) technology that uses Fortezza cards for personnel identification and encryption services.

BACKGROUND INFORMATION

The DMS program began in 1989, with the Defense Information Systems Agency developing target architecture and later engaging the Air Force as the component acquisition manager. In 1992, the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence issued a policy mandating the transition to, and use of, DMS compliant systems. In March 1995, additional policy guidance imposed a moratorium on the acquisition of non-DMS compliant electronic messaging systems. In August of 1997, IOT&E of DMS Release 1.0 revealed promise, but DMS could not yet adequately support many critical requirements. In March-April 1998, a Limited User Field Test of DMS 1.1 reassessed IOT&E measures and tested some additional capabilities. Although the Limited User Field Test demonstrated significant improvement, five of the nine “most critical” measures of performance did not meet their criteria. Again, DMS did not adequately exchange messages with non-DMS users or reroute traffic around failed elements; no site was able to install DMS and setup operations without the assistance of contractors; and no site achieved the laboratory-tested secure configuration against information warfare attacks. Since commitments were made to severely downsize AUTODIN by December 1999, the Joint Staff pressed for significant improvements and OT&E of DMS 2.1 to base their transition planning. To fully implement DSM requires replacing AUTODIN, supporting Allied Communications Publications (ACP) 120 message standards, and Service and Agency implementation of tactical and intelligence elements. These efforts will take several years and involve several more operational tests.

TEST & EVALUATION ACTIVITY

The Joint Interoperability Test Command (JITC) led a joint test team composed of each of the Service’s operational test agencies. They executed the joint OT&E of DMS Release 2.1 in September 1999 according to a new and fully coordinated DMS Capstone TEMP approved on July 1, 1999. OT&E of DMS 2.1 evaluated the same critical operational issues as all previous operational tests: (1) messaging services; (2) directory services; (3) security; (4) survivability; (5) suitability; and (6) usability. OT&E was conducted at four principal sites, one from each Service, one of which was overseas and U.S. Central Command. It also included dial-in users and interfaces with AUTODIN, tactical, allied, and simple email users. Other test improvements included more independent developmental testing and two pilot tests at the operational test sites to ensure readiness for full OT&E.

Due to the DoD-wide scope of DMS, its test limitations contained lessons for the entire Defense Information Infrastructure (DII). For example, it is impractical to load the Defense Information Infrastructure backbone communications to a wartime stress just for DMS; however, this backbone has never been evaluated at a full wartime load. Different sites have different network configurations and levels of system administration support, so testing at only four sites is an obvious limitation even for the initial 250-site DMS implementation. A final example of a lesson learned from this is information warfare (IW) testing of DMS. This testing proceeded in a standard fashion targeted at gaining “root control” over DMS infrastructure computers and, in an effort to save time, testers were given free access through firewalls. However, this generic IW testing approach erodes the persuasiveness of the results for two reasons. First, it does not

evaluate the DII layers of security protections and second, it does not target the specific functions of the systems under test. For example, no attempt was made to compromise encrypted DMS messages.

TEST & EVALUATION ASSESSMENT

During OT&E, DMS 2.1 showed remarkable improvement compared with previous releases—all but one of six critical operational issues were resolved satisfactorily. The operational testers evaluated DMS 2.1 as operationally suitable but not effective. All but four of fourteen critical measures of performance met the criteria established by the Joint Staff. Three of the remaining deficiencies were caused by either the inability of AUTODIN to deliver messages after successfully receiving them from DMS or by immature tracing procedures within DMS and between DMS and AUTODIN. The final critical measure, safeguards from altering security protections, did not meet its criterion because the information warfare test team was able to penetrate all but one test site with only a moderate level of effort. The obvious reason for this serious deficiency was that system administrators were unable to set up and configure DMS securely. However, the underlying factors are the complexity of DMS, the need to reconfigure DMS to integrate it with each distinct site's supporting architecture, and the lack of automated aids to check DMS security posture once it is installed or after it is reconfigured.

DOT&E concurs with the joint test team's evaluation of DMS 2.1 as not operationally effective due to its security deficiencies. However, we differ with the joint test team on suitability and evaluate DMS 2.1 as also not operationally suitable. While the joint test team based their evaluation on the fact that DMS 2.1 did not fail any suitability COIs, we base our evaluation of suitability on the combined effect of several less critical deficiencies. As revealed by the OT&E, the typical system administrator is not equipped to install, upgrade, maintain, troubleshoot, or recover DMS 2.1 from crashes. These weaknesses may also have led to the security deficiency. Skilled installation specialist teams, as well as better training, documentation, system administrator tools, and help desks could mitigate some aspects of these suitability deficiencies. However, other aspects require broader skills, more personnel, and better tools than currently available to support DMS. Since the expected migration of users from AUTODIN to DMS will rapidly increase the pressures on system administrators, DOT&E judges the supportability problems exhibited during OT&E of DMS 2.1 as symptomatic of potentially more serious difficulties to come. The lack of qualified system administrators to operate and maintain critical UNIX-based systems such as DMS is a DoD-wide issue that needs to be addressed by every Service, CINC, and Agency.

CONCLUSIONS, RECOMMENDATIONS, LESSONS LEARNED

DOT&E concurs with the decision to field DMS 2.1 after implementing a security improvement and monitoring program and taking corrective actions to enhance installation and supportability. Our view is based on the belief that:

- DoD messaging must continue to employ commercial products and be compatible with commercial standards.
- DMS 2.1 is much better than alternative options.
- Expanded user operational experience with less sensitive missions is the best means of exploring the scope of system administration and supportability requirements.

Observations of DMS meeting its operational measures during laboratory, beta testing, and pilot operational testing before going into the operational test, identified many obvious problems and enabled the developer to correct them so that full OT&E addressed the more suitable and substantive aspects of performance. In fact, the operational user commented that the requirement to execute full OT&E was clearly responsible for the remarkable improvement of DMS 2.1 over the several previous releases subjected to only operational assessments.

The DMS program, in coordination with Services and Agencies, should invest in more basic system support and security areas. To some extent this depends on better user-defined policies and procedures, but developers should also try to ease the burdens of system administration, directory management, and security administration through management simplification, automated aids, streamlined procedures, more usable documentation, improved training, and more capable help desks. Since future DMS releases will incorporate higher security levels, more automated interfaces, and management tasks, it is imperative that they begin minimizing the administrative burden.

Three principal problem areas of the Defense Message System and the Defense Information Infrastructure in general are information assurance, system administration, and stability under wartime stresses. Recognition of these problems has already supported the creation of the Global Information Grid to replace the Defense Information Infrastructure. Since DMS is the most complicated system to ride on the Defense Information Infrastructure, DMS OT&E could reveal problems that range far beyond the scope or control of the DMS program itself. While it is inappropriate to delay the DMS program for the known weaknesses of the operational Defense Information Infrastructure, it is equally essential to conduct wider-scale, more realistic tests of these critical Defense Information Infrastructure capabilities.