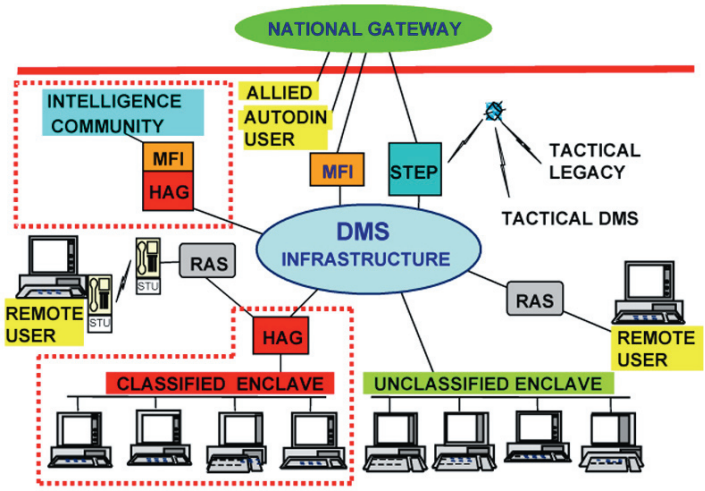
# Defense Message System (DMS)

### Executive Summary

- The Defense Message System (DMS) 3.0 achieved full fielding approval for the DoD General Service messaging community in July 2002.
- The Joint Interoperability Test Command conducted an operational assessment of DMS 3.1 in May 2005. DMS 3.1 is not operationally effective or suitable.
- The Air Force Information Warfare Center conducted a vulnerability assessment in conjunction with the operational assessment. Many security vulnerabilities were identified both at the infrastructure and site level.
- A follow-on test is required after all major deficiencies identified during the operational assessment are fixed.

### System

- DMS is the messaging component of the DoD Global Information Grid. DMS consists of all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between organizations and individuals in the DoD. DMS also includes the interfaces to the messaging systems of other government agencies, allies, defense contractors, and other approved organizations.
- DMS is a secure and accountable writer-to-reader messaging system.
- DMS is to replace the legacy Automatic Digital Network organizational messaging system. During the transition, DMS uses the Multi-Function Interpreter as the primary means of providing interoperability with the Automatic Digital Network. For messages across security domains (e.g., Secret and unclassified), DMS uses the High Assurance Guard to provide secure guard services. DMS users interface with tactical users through the Standard Tactical Entry Point.
- Some communities (e.g., small deck Navy ships, non-DoD federal departments, allies, and defense contractors) will continue to operate their legacy messaging systems using the National Gateway Center to communicate with each other and to interface with DMS.




### Mission

- DoD users, including deployed tactical forces, use DMS to exchange both classified and unclassified messages.
- DMS also enables DoD users to interface with allies, other government agencies, defense contractors, and other approved activities outside of DoD.

### Activity

- DMS 3.0 received full fielding approval for the DoD General Service messaging community in July 2002. Operational test results showed that the system performed well overall with deficiencies in the information assurance area. System administrators had failed to protect all system elements, attributable primarily to poor security password and system administration practices.
- In May 2005, the Joint Interoperability Test Command led a multi-Service and agency test team in an operational assessment of DMS 3.1. DMS 3.1 provided an upgraded commercial software baseline among other enhancements, including enhanced originator requested alternate recipient capabilities. Concurrent with the operational assessment, the Air Force Information Warfare Center conducted a vulnerability assessment.
- Operational testing has been done in accordance with the DOT&E-approved Test and Evaluation Master Plan and test plans.

### Assessment

DMS 3.1 is not operationally effective or suitable as tested in May 2005. Test results revealed that DMS message delivery was mostly successful using the classic DMS products. However, sites using the new DMS core products of the automated Message Handling System and/or Defense Message Dissemination System showed unacceptable performance. Furthermore, DMS messaging to the legacy and allied systems through the Multi-Function Interpreter did not perform well during the test. Message traces indicated a high percentage of messages lost or timed-out in the legacy systems. Messaging between unclassified

and Secret security enclaves also exhibited difficulties mostly due to the operations of the Tactical Guard, which prevented successful message exchanges across the security enclaves.

Vulnerability assessment results showed that there were many deficiencies that existed at both the infrastructure and site level. Noted vulnerabilities included:

- Software security patches and service packs were outdated or missing.
- Weak, null, or default passwords were being used.
- Excessive file and directory permissions.
- Unnecessary services and/or applications were allowed.
- Clear text protocols were used.
- Inconsistent account management policies across the sites.

**Recommendations**

1. DMS 3.1 fielding should not commence until all major deficiencies identified during the operational assessment are fixed and corrections are verified by the operational testers in a follow-on test.
2. Identified security deficiencies that DMS does not have direct control over should be referred to the user sites directly for remediation.