



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

November 12, 2003

MEMORANDUM FOR DIRECTOR, DEFENSE LOGISTICS AGENCY

SUBJECT: Report on Defense Logistics Agency Information Assurance Investment Initiative (Report No. D-2004-019)

This is our report on the audit of the Defense Logistics Agency (DLA) Information Assurance Investment Initiative for your review. We performed the audit under Project No. D2002AS-0165 and based on issues identified during the audit of a Hotline allegation on information assurance management at the Defense Logistics Agency. We substantiated the allegation and issued Report No. D-2003-080, "Allegations Concerning Information Assurance Management at the Defense Logistics Agency," April 21, 2003.

The objective of this audit was to determine whether DLA complied with statutory and regulatory acquisition requirements for its information assurance (IA) investment initiatives. Specifically, we reviewed the IA investment initiative for automating the DLA System Security Authorization Agreement (SSAA) preparation process. We did not review the management control program related to the overall objective because DoD designated information assurance as a systemic management control weakness in the FY2002 Performance and Accountability Report.

We performed the audit from July 2002 through November 2003 in accordance with generally accepted government auditing standards. The DLA IA investment initiative for automating the SSAA process, now called the Enterprise Mission Assurance Support System (eMASS), evolved from the Comprehensive Information and Assurance Knowledge Base. To assess the SSAAs that DLA developed using the automated process, we judgmentally selected seven DLA field sites and reviewed 13 SSAAs that were prepared between October 2000 and January 2003. Also we verified the documentation and processes supporting the certification and accreditation (C&A) of systems, networks, and Web sites included on the SSAAs reviewed.

DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997 and DoD Manual 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process Manual, (DITSCAP manual)" July 31, 2000, establish a standard process and management structure to identify all IA requirements and solutions within the SSAA. According to DITSCAP policy, the SSAA documents the conditions of C&A for an information technology system. In addition to providing an automated process for SSAA preparation, eMASS electronically maintains SSAAs and tracks the C&A status of DLA systems, networks, and Web sites. According to DLA officials, as of November 2003, DLA had obligated approximately \$9 million to develop and implement eMASS.

During the audit, we identified issues for the DLA C&A process in the areas of independent assessment, threat assessment, and risk assessment. DLA took corrective actions to resolve those issues. We also identified where DLA could better use the eMASS capability in documenting the C&A validation process. Our comments on the DLA C&A process and the validation documentation are discussed below.

DLA C&A Process. Initially, the DLA C&A process did not follow DITSCAP requirements for independent assessment, threat assessment, and risk assessment. However, the DLA IA Program Manager revised the DLA C&A process to incorporate the DITSCAP policy requirements for C&A into the SSAA preparation process. We commend the Program Manager for enhancing the C&A process for the DLA systems, networks, and Web sites. The specific actions the Program Manger took to enhance the C&A process follows.

Independent Assessment. DITSCAP policy requires information system professionals to analyze system-related factors to determine the level of effort required to certify an IT asset level of effort, which range from using a minimum security checklist to evaluate the asset to using an extensive independent analysis. Additionally, DITSCAP policy requires information system professionals to maintain independence when determining the certification level of effort to ensure that the accreditation decision is supported by the most objective information available. Our review of the DLA SSAA preparation process showed that DLA did not require an independent assessment of system factors to determine the certification level of effort. However, as of February 2003, the IA Program Manager updated the C&A process to require that personnel to assess system factors to determining the certification level of effort for C&A be independent of systems, networks, and Web sites assessed.

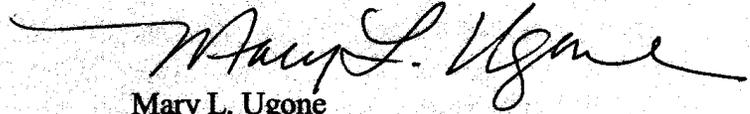
Threat Assessment. DITSCAP policy requires information system professionals to assess any circumstance or event that has the potential to harm an information system. The policy also requires information system professionals to tailor generic threat information to clearly state the expected threat and, where possible, the expected frequency of occurrence of threat to the information system. Initially, the IA Program Manager allowed personnel to provide generic threat information that did not address specific expected threat or the expected frequency of occurrence. As of February 2003, the IA Program Manager updated the C&A process to require personnel to provide threat assessments that address the potential impact on availability, confidentiality, and integrity of system-specific threats.

Risk Assessment. In addition to threat assessment requirements, DITSCAP policy requires information system professionals to perform a risk assessment to analyze threats and vulnerabilities and the potential impact that the loss of information or system capabilities would have on national security. Initially, the IA Program Manager included a list of controls to assess system vulnerabilities but did not the address potential harm or perceived threat to the systems, networks, and Web sites. As of February 2003, the IA Program Manager updated the C&A process to require the tailoring of the corporate risk assessment to identify system-specific missions, threats, and risks.

Validation Documentation. DITSCAP policy requires the certification team to prepare a test plan that identifies the methodology and results of the actual test. Although, eMASS has the capability for the tester to record actual test methodology and results data, DLA does not require the tester to enter that data. Without documenting the methodology and results used to validate security features, DLA cannot provide assurance of adequate testing, correct operation of security features, or the security posture of information technology assets. Although information on the C&A process could become voluminous, documenting the security-related efforts conducted to validate the proper operation of all security features provides reasonable assurance that DLA knew the risk that it assumed or mitigated when it granted authority for assets to operate in a network environment.

This report does not contain recommendations; therefore, no written response to this report is required. We appreciate the courtesies extended to the audit staff. Questions should be directed to Ms. Wanda A. Scott at (703) 604-9049 (DSN 664-9049) and Ms. Dianna J. Pearson at (703) 604-9063 (DSN 664-9063).

By direction of the Deputy Inspector General for Auditing:



**Mary L. Ugone
Director
Acquisition Management Directorate**

**cc: Under Secretary of Defense Acquisition, Technology, and Logistics
Assistant Secretary of Defense for Networks and Information Integration/DoD Chief
Information Officer**