GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-06-31, a report to congressional committees

October 2005

INFORMATION SECURITY

The Defense Logistics Agency Needs to Fully Implement Its Security Program

Why GAO Did This Study

The Defense Logistics Agency's (DLA) mission is, in part, to provide food, fuel, medical supplies, clothing, spare parts for weapon systems, and construction materials to sustain military operations and combat readiness. To protect the information and information systems that support its mission, it is critical that DLA implement an effective information security program. GAO was asked to review the efficiency and effectiveness of DLA's operations, including its information security program. In response, GAO determined whether the agency had implemented an effective information security program.

What GAO Recommends

To assist DLA in fully implementing its security program, GAO is making recommendations to the Secretary of Defense to direct the DLA Director to take several actions to fully implement key information security practices and controls.

In commenting on a draft of this report, the Department of Defense agreed with most of GAO's recommendations and described efforts to address them. However, the department disagreed with recommendations related to annual security testing and evaluation, verification of certification tasks, and the accuracy of performance data in DLA's reporting tool.

www.gao.gov/cgi-bin/getrpt?GAO-06-31.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Although DLA has made progress in implementing important elements of its information security program, including establishing a central security management group and appointing a senior information security officer to manage the program, it has not yet fully implemented other essential elements. For example, the agency did not consistently assess risks for its information systems; sufficiently train employees who have significant information security responsibilities or adequately complete training plans; annually test and evaluate the effectiveness of management and operational security controls; or sufficiently complete plans of action and milestones for mitigating known information security deficiencies. The table below indicates with an "X" weaknesses in the implementation of key information security practices for the 10 DLA systems that GAO reviewed.

Weaknesses in Information Security Practices and Controls

DLA system[a]	Risk assessment	Security training and awareness plan	Security test and evaluation	Plans of action and milestones
1	X		X	X
2				X
3	X	X	X	X
4	X		X	X
5	X		X	X
6	X	X	X	X
7	X		X	X
8	X		X	X
9	X		X	X
10	X	X	X	X

Source: GAO analysis of information security documentation for selected systems.

[a] The systems selected consisted of local area networks and Web sites that support a DLA location; production systems, such as those that form the bulk of the computing environment at a DLA location; or an information system that has been replicated with the same configuration and has been deployed at multiple locations.

In addition, DLA has not implemented a fully effective certification and accreditation process for authorizing the operation of its information systems.

Key reasons for these weaknesses are that responsibilities of information security employees were not consistently understood or communicated and DLA has not adequately maintained the accuracy and completeness of data contained in its primary reporting tool for overseeing the agency's performance in implementing key information security activities and controls. Until the agency addresses these weaknesses and fully implements an effective agencywide information security program, it may not be able to protect the confidentiality, integrity, and availability of its information and information systems, and it may not have complete and accurate performance data for key information security practices and controls.