United States Government Accountability Office

GAO

Report to Congressional Committees

October 2005

INFORMATION SECURITY

The Defense Logistics Agency Needs to Fully Implement Its Security Program



GAO-06-31

October 2005

INFORMATION SECURITY

The Defense Logistics Agency Needs to Fully Implement Its Security Program

GAO Accountability · Integrity · Reliability

Highlights

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

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.

Contents

Letter 1

Results in Brief 2
Background 4
DLA Has Not Yet Fully Implemented Its Security Program 9
Conclusions 19
Recommendations for Executive Actions 20
Agency Comments and Our Evaluation 21

Appendixes

Appendix I: Scope and Methodology 25
Appendix II: Comments from the Department of Defense 27
Appendix III: GAO Contact and Staff Acknowledgments 32

Tables

Table 1: Weaknesses in Information Security Practices and Controls 10
Table 2: Percentage of DLA Locations and Systems Subjected to Program Reviews During the Last 3 Years 15

Figure

Figure 1: Simplified Overview of the Defense Logistics Agency's Information Assurance Management and Reporting Structure 7

Abbreviations

DOD	Department of Defense
DLA	Defense Logistics Agency
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

October 7, 2005

The Honorable John Warner
Chairman
The Honorable Carl Levin
Ranking Minority Member
Committee on Armed Services
United States Senate

The Honorable Duncan L. Hunter
Chairman
The Honorable Ike Skelton
Ranking Minority Member
Committee on Armed Services
House of Representatives

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission. It is especially important for government agencies, where maintaining the public's trust is essential. Federal agencies face increasing security risks from viruses, hackers, and others who seek to disrupt federal operations or obtain sensitive information that is stored in federal computers. In our reports to Congress since 1997—most recently in January 2005[1]—we have identified information security as a governmentwide high-risk issue.

The Defense Logistics Agency (DLA) relies extensively on information systems in supporting America's military forces with food, fuel, medical supplies, clothing, spare parts for weapons systems, and construction materials. To protect the information and information systems that support its operations and assets, it is critical that DLA implement an effective information security program. Recognizing that the major underlying cause for the majority of information security problems in federal agencies is the lack of an effective information security program, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which set forth a comprehensive framework for ensuring the effectiveness of information security controls over the information resources that support federal operations and assets.

[1]GAO, *High Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

The National Defense Authorization Act for Fiscal Year 2001 required us to review the efficiency and effectiveness of DLA's operations. In response to this mandate, we previously evaluated the effectiveness of information system general controls[2] at one of DLA's critical business support units and reported significant findings, conclusions, and recommendations in a "limited official use only" report in January 2004. As agreed with your offices, the objective for this review was to determine whether DLA has implemented an effective agencywide information security program.

We performed our review at DLA facilities in the Washington, D.C. metropolitan area; Columbus, Ohio; and Denver, Colorado, from September 2004 to July 2005 in accordance with generally accepted government auditing standards. Details of our scope and methodology are contained in appendix I.

Results in Brief

DLA has not yet fully implemented an effective agencywide information security program to protect the information and information systems that support its operations and assets. While DLA has implemented important elements of its information security program—including establishing a central security management group, appointing a senior information security officer to manage the program, and ensuring that employees and contractors receive information security awareness training—it has not yet fully implemented other elements of its program. Specifically, risks that could result from the unauthorized access, use, disclosure, or destruction of information or information systems were not consistently assessed; employees who had significant information security responsibilities did not receive sufficient training, and security training plans sometimes lacked key information; security testing and evaluation of management and operational controls were not annually performed; and plans of action and milestones for mitigating known information security deficiencies were not sufficiently completed. In addition, DLA has not implemented a fully

[2]Information system general controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. These controls include security management, operating procedures, software security features, and physical protection designed to ensure that access to data is appropriately restricted, computer security functions are segregated, only authorized changes to computer programs are made, and backup and recovery plans are adequate to ensure the continuity of essential operations.

effective certification[3] and accreditation[4] process for authorizing the operation of its information systems.

Key reasons for these weaknesses are that the responsibilities of key information security employees were not consistently understood or communicated and DLA has not maintained the accuracy and completeness of the data contained in its central management database—the primary reporting tool for managing and overseeing the agency's performance in implementing key information security activities and controls. Until DLA 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.

To assist DLA in fully implementing its information security program, we are 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, including strengthening the process for certifying and accrediting information systems, and maintaining the accuracy and completeness of the data contained in DLA's primary reporting tool.

In providing written comments on a draft of this report, the Deputy Under Secretary of Defense (Business Transformation) agreed with 7 of our 10 draft recommendations and described ongoing and planned efforts to address them. For the remaining recommendations, however, the Deputy Under Secretary gave reasons for the department's disagreement that did not address the intent of our recommendations. Accordingly, we have revised our draft recommendations to make our intent clear. Written comments from the Deputy Under Secretary of Defense (Business Transformation) are reprinted in appendix II.

[3]Certification is a comprehensive evaluation of security controls that provides the necessary information for a designated approving authority to formally declare that a system is approved to operate at an acceptable level of risk.

[4]Accreditation is the authorization of an information system to process, store, or transmit information that provides a form of quality control. The accreditation decision is to be based on the implementation of an agreed-upon set of management, operational, and technical controls for a system and is supported by a comprehensive evaluation or certification of these security controls that provides the necessary information for a designated approving authority to formally declare that a system is approved to operate.

Background

The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. Because of the concern about attacks from individuals and groups, protecting the computer systems that support critical operations and infrastructures has never been more important. These concerns are well founded for a number of reasons, such as escalating threats of computer security incidents, the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks. According to experts from government and industry, during the first quarter of 2005, more than 600 new Internet security vulnerabilities were discovered, thereby placing organizations that use the Internet at risk.

Computer-supported federal operations are likewise at risk. IBM recently reported that there were over 54 million attacks against government computers from January 2005 to June 2005.[5] Without proper safeguards, there is risk that individuals and groups with malicious intent may intrude into inadequately protected systems and use this access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. How well federal agencies are addressing these risks is a topic of increasing interest in both Congress and the executive branch. This is evidenced by recent hearings on information security intended to strengthen information security.[6]

DLA Is a Major Defense Supplier

DLA is an agency of the Department of Defense (DOD). As DOD's supply chain manager, DLA provides food, fuel, medical supplies, clothing, spare parts for weapon systems, and construction materials to sustain DOD military operations and combat readiness. To fulfill its mission, DLA relies extensively on interconnected computer systems to perform various functions, such as managing about 5.2 million supply items and processing

[5]IBM, *Security Threats and Attack Trends Report*: January 2005 to June 2005.

[6]GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*, GAO-05-827T (Washington, D.C.: July 19, 2005); GAO, *Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks*, GAO-05-845T (Washington, D.C.: June 29, 2005); and GAO, *Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements*, GAO-05-483T (Washington, D.C.: April 7, 2005).

about 54,000 requisition actions per day for goods and services. DLA employs about 22,575 civilian and military workers, located at about 500 field locations in 48 states and 28 countries.

In accordance with DOD policy,[7] DLA has developed an agencywide information security program to provide information security for its operations and assets. The DLA Director is responsible for ensuring the security of the information and information systems that support the agency's operations. In carrying out this responsibility, the Director has delegated to DLA's chief information officer the authority to ensure that the agency complies with FISMA and with other information security requirements.

DLA's chief information officer has also designated a senior agency official to serve as Director of Information Assurance—the agency's senior information security officer—and to head the central security management group, commonly referred to as the information assurance program office. This group carries out specific responsibilities, including the following:

- documenting and maintaining an agencywide security framework to assess the agency's security posture, identify vulnerabilities, and allocate resources;

- establishing and managing security awareness and specialized professional security training for employees who have significant security responsibilities;

- ensuring that all systems are certified and accredited in accordance with both federal and DOD processes;

- providing personnel at headquarters and the DLA locations with guidance on, and assistance in preparing, system security authorization agreements—single source data packages for all information pertaining to the certification and accreditation of a system in order to, among other things, guide actions, document decisions, specify information security requirements, and maintain operational systems security; and

[7]DOD Directive 8500.1, *Information Assurance* (Washington, D.C.: October 2002); and DOD Instruction 8500.2, *Information Assurance Implementation*, (Washington, D.C.: February 2003).

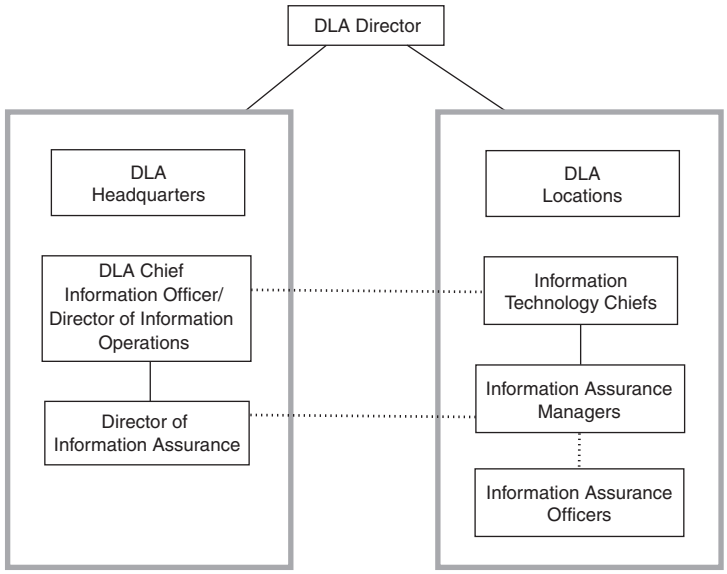
- ensuring that field site personnel accurately assess their locations' security postures.

Information assurance managers at the various DLA locations directly report to the information technology chief at their location and are expected to assist the Director of Information Assurance by coordinating security activities, establishing and maintaining a repository for documenting and reporting system certification and accreditation activities, maintaining and updating system security authorization agreements, and notifying the designated approving authority[8] of any changes that could affect system security.

Information assurance officers at the various DLA locations assist the information assurance managers through the following activities: ensuring that appropriate information security controls are implemented for an information system, notifying the information assurance manager when system changes that might affect certification and accreditation are requested or planned, and conducting annual validation testing of systems. Figure 1 below shows a simplified overview of DLA's information assurance management and reporting structure.

[8]A designated approving authority is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, assets, or individuals.

Figure 1: Simplified Overview of the Defense Logistics Agency's Information Assurance Management and Reporting Structure



Source: GAO analysis of information provided by DLA.

Federal and Departmental Requirements Are to Guide DLA Information Security Activities

Congress enacted FISMA to strengthen the security of information and information systems within federal agencies. FISMA requires each agency to develop, document, and implement an agencywide information security program to protect the information and information systems that support the operations and assets of the agency—including those that are provided or managed by another agency, a contractor, or some other source. The program must include the following:

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, modification, disruption, or destruction of information or information systems;
- training of personnel who have significant responsibility for information security and security awareness training to educate personnel—including contractors and other users of the agency's information systems—about information security risks and their responsibilities to comply with the agency's security policies and procedures;

- periodic testing and evaluation of the effectiveness of the agency's information security policies, procedures, and practices; and

- a process for planning, implementing, evaluating, and documenting plans of action and milestones that are taken to address any deficiencies in the agency's information security policies, procedures, and practices.

To support agencies in conducting their information security programs, the National Institute of Standards and Technology (NIST) is publishing mandatory standards and guidelines for providing information security all agency operations, assets, and information systems other than national security systems.[9] The standards and guidelines include, at a minimum, (1) standards to be used by all agencies to categorize their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels, (2) guidelines recommending the types of information and information systems that are to be included in each category, and (3) minimum information security requirements for information and information systems in each category.

In addition, DOD has developed and published various directives and instructions that comprise an information assurance policy framework that is intended to meet the information security requirements specified in FISMA and NIST standards and publications. This framework applies to all of DOD's systems—both national and non-national security systems—including those operated by or on behalf of DLA. DLA's policies and procedures for implementing its agency information security program are contained in DLA's One Book policy and agency handbook.

[9]44 U.S.C. 3542(b)(2).

DLA Has Not Yet Fully Implemented Its Security Program

DLA has implemented important elements of an information security program—including establishing a central security management group, appointing a senior information security officer to manage the program, and providing security awareness training for its employees. However, DLA has not yet fully implemented other essential elements of an effective information security program to protect the confidentiality, integrity, and availability of its information and information systems that support its mission. Collectively, these weaknesses place DLA's information and information systems at risk. Key underlying reasons for the weaknesses pertain to DLA's management and oversight of its security program.

DLA Has Implemented Important Elements of Its Security Program

In carrying out their information security responsibilities, both the Chief Information Officer and the Director of Information Assurance have taken several steps to implement important elements of DLA's security program, including the following:

- ensuring employees and contractors receive information security awareness training;
- developing information security procedures and guidance for use in implementing the requirements of the program;
- deploying information system security engineers to assist headquarters and field staff in implementing security policies and procedures consistently across the agency;
- developing an agencywide management tool—known as the Comprehensive Information Assurance Knowledgebase—to centrally manage and report on key performance measures, such as the status of security training, plans of action and milestones, and certification and accreditation activities; and
- developing and implementing various automated information technology initiatives to assist information assurance managers and information assurance officers in improving DLA's security posture.

Weaknesses Place DLA's Information and Information Systems at Risk

Weaknesses in information security practices and controls place DLA's information and information systems at risk. Our analysis of information security activities for selected systems at 10 DLA locations showed that the agency had not fully or consistently implemented important elements of its program. Specifically, risks that could result from the unauthorized access, use, disclosure, or destruction of information or information systems were not consistently assessed; employees who had significant information security responsibilities did not receive sufficient training, and security training plans were sometimes not adequately completed; testing and evaluation of the effectiveness of management and operational security controls were not adequately performed; and plans of action and milestones for mitigating known information security deficiencies were not sufficiently completed. Table 1 indicates with an "X" weaknesses in the implementation of key information security practices and controls for selected systems.

Table 1: 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 contained in system certification and accreditation packages.

[a]The 10 systems selected consist 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 have been replicated with the same configuration and have been deployed at multiple locations.

DLA Did Not Assess Risks Consistently

FISMA requires that agencies' information security programs include periodic assessments of the risk and magnitude of the harm that could

result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. Identifying and assessing information security risks are essential steps in order to determine what controls are required and what level of resources should be expended on these controls. NIST has developed guidance to help organizations protect their information and information systems by using security controls that are selected through a risk-based process.

DOD established a set of baseline security controls[10] for each of three mission assurance categories[11] that determine what security controls should be implemented. These controls are adjusted based on an assessment of risk including specific threat information, vulnerabilities, and countermeasures relative to the system. Vulnerabilities that are not mitigated are referred to as residual risk. The designated approving authority considers the residual risks in determining whether to accredit a system. Such risk assessments, as part of the requirement to reaccredit systems, are to be performed prior to a significant change in processing, but at least every 3 years.

Although DLA categorized its systems in accordance with DOD guidance, we found that it did not consistently assess the residual risk for 9 of the 10 systems we selected for review. For example:

- nine did not use the established baseline security controls to assess the residual risk;
- three did not clearly identify the threats, vulnerabilities, and countermeasures;
- two did not state how the threats and vulnerabilities would affect the mission that the system supports;

[10]DOD Instruction 5200.40, *DOD Information Technology Security Certification and Accreditation Process (*December 30, 1997); DOD 8510.1-M, *DOD Information Technology Security Certification and Accreditation Process Application Manual* (July 31, 2000); and DOD Instruction 8500.1, *Information Assurance (*October 24, 2002).

[11]Mission assurance category (MAC) I are systems designated as vital to the operational readiness or mission effectiveness and their loss would be unacceptable. MAC II are systems designated as important in the support of deployed or contingency forces and their loss are unacceptable. MAC III are systems designated as necessary for the conduct of day-to-day business and their loss could be tolerated or overcome without significant impact.

- one only referenced the security controls as the threat or vulnerability; and

- one had not been updated since 2001.

Unless DLA performs risk assessments consistently and assesses them against the appropriate set of controls, it will not have assurance that it has implemented appropriate controls that cost-effectively reduce risk to an acceptable level.

Employees Did Not Receive Sufficient Training and Security Training Plans Were Sometimes Incomplete

FISMA mandates that all federal employees and contractors who are involved in the use of agency information systems be provided training in information security awareness and that agency heads ensure that employees with significant information security responsibilities are provided sufficient training with respect to such responsibilities. An effective information security program should promote awareness and provide training so that employees who use computer resources in their day-to-day operations understand security risks and their roles in implementing related policies and controls to mitigate those risks. DOD guidance requires that individuals receive the necessary training to ensure that they are capable of conducting their security duties and that each component establish and implement information assurance training and professional certification programs. DOD also requires that security awareness and training plans be documented for each system as part of the certification and accreditation process. These security training plans specify that training for individuals associated with a system's operation be appropriate to an individual's level and area of responsibility. This training should provide information about the security policy governing the information being processed, as well as potential threats and the nature of the appropriate countermeasures.

DLA provided annual security awareness training for employees and contractors for whom it was appropriate. However, employees with significant information security responsibilities did not receive sufficient training. For example, of the 17 information assurance managers and information assurance officers located where we reviewed selected systems:

- eleven reported having received some form of training, although eight of them had received training on only one of their security responsibilities—developing security documentation;

- six reported never having received any security training; and
- two reported having received no security training for 2 or more years.

Further, security training and awareness plans for 3 of the 10 systems we reviewed were either not system-specific or lacked detailed information. For example, training plans for 2 systems did not specify, for each level and area of responsibility, the system operations appropriate for a given user. The third lacked detailed information about training objectives, goals, and requirements.

A key reason for these weaknesses is that the individual responsible for monitoring the agency's security training program had other significant responsibilities and was not able to effectively ensure that employees received the required training. As a result, DLA does not have assurance that employees with significant security responsibilities are equipped with the knowledge and skills they need to understand information security risks and their roles and responsibilities in implementing related policies and controls to mitigate those risks.

Security Testing and Evaluation of Management and Operational Controls Were Not Annually Performed

Another key element that FISMA requires of an information security program is periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency based on risk, but not less than annually. FISMA requires that such testing and evaluation activities shall include the management, operational, and technical controls[12] of every system identified in an agency's information systems inventory.[13]

DOD policy requires periodic reviews of operational systems at predefined intervals.[14] Such reviews include testing and evaluating the technical

[12]Management controls focus on the management of the system and the risk of harm to a system. Operational controls address security methods, implemented and executed by people (as opposed to systems), to improve the security of a particular system or group of systems. They often require technical or specialized expertise and often rely on management activities as well as technical controls. Technical controls focus on security controls that the computer system executes. These controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

[13]Section U.S.C. 3544(b)(5).

[14]DOD Instruction 5200.40, December 30, 1997.

implementation of the security design of a system and ascertaining that security software, hardware, and firmware features affecting the confidentiality, integrity, availability, and accountability of information and information systems have been implemented and documented. The results of testing and evaluation of security controls are to be used in the decision-making process for authorizing systems to operate. Further, DLA's One Book policy requires information assurance managers and information assurance officers to use the security test and evaluations as the method for validating the adequacy of management, operational, and technical controls, at least annually.

DLA did not annually test and evaluate the management and operational security controls of its systems. According to DLA officials, vulnerability scans[15] and information assurance program reviews[16] collectively satisfied the annual requirement for testing and evaluating management, operational, and technical controls. However, the combination of the vulnerability scans and the program reviews did not satisfy the annual requirement. Although DLA generally assessed technical controls by conducting annual vulnerability scans on its systems, it did not annually assess the management and operational controls for each of its systems. While the program reviews are intended to satisfy the requirement for testing and evaluating the management and operational controls, DLA does not conduct these reviews annually on every system. For example, less than half of DLA's locations and systems have undergone program reviews in the last 3 years, as shown in table 2.

[15]Vulnerability scans assess certain technical controls, such as vulnerable services, and are conducted annually to identify the weaknesses of computing systems in order to determine whether and where a system can be exploited and/or threatened.

[16]Information assurance program reviews are generally conducted on a 3-year cycle to evaluate the effectiveness of management, operational, and technical controls agencywide through assessment of security program management certification and accreditation information, network security policies and practices, vulnerability assessment, compliance and configuration, and incident response reporting and handling.

Table 2: Percentage of DLA Locations and Systems Subjected to Program Reviews During the Last 3 Years

System category	Percent
Vital to operations	43
Important in support of military forces	26
Necessary for day-to-day operations	8

Source: GAO analysis of DLA data.

Until DLA tests and evaluates management and operational controls annually, critical systems may contain vulnerabilities that have not been identified or appropriately considered in decisions to authorize systems to operate. Moreover, DLA may not be able to ensure the confidentiality, integrity, and availability of the sensitive data that its systems process, store, and transmit.

Plans of Action and Milestones Were Incomplete

FISMA requires each agency to develop a process for planning, implementing, evaluating, and documenting remedial action plans to address any deficiencies in its information security policies, procedures, and practices. Developing effective corrective action plans is key to ensuring that remedial action is taken to address significant deficiencies. The Office of Management and Budget (OMB) requires agency chief information officers to document and report all agency information assurance weaknesses and remedial actions in plans of action and milestones. The plans should list each security weakness and the tasks, resources, milestones, and scheduled completion dates for remedying each weakness.

The plans of action and milestones associated with the 10 systems we selected for review were incomplete. For example:

- none of the plans clearly documented and reported the nature of the weakness being addressed;
- seven did not identify the start or completion dates for addressing the weakness;
- none specified the resources necessary to complete the action plan;
- nine did not list the risk associated with the security weakness;

- six were not based on the correct set of baseline security controls; and
- one plan contained steps to identify vulnerabilities rather than the steps required to remedy vulnerabilities.

A key reason for these weaknesses is that information assurance managers and information assurance officers reported that they did not understand the requirements for reporting system security vulnerabilities because DLA had not provided specific criteria or instructions on what—or how—to document and report plans of action and milestones for system deficiencies. Having reliable plans of action and milestones is not only vital to ensuring that DLA's information and information systems receive adequate protection, but it is also important for accurately managing and reporting progress on them. Without reliable plans, DLA does not have assurance that all information security weaknesses have been reported and that corrective actions will be taken to appropriately address the weaknesses.

Certification and Accreditation Process Was Not Fully Effective for Authorizing Systems

OMB requires that agencies establish a certification and accreditation process for formally authorizing systems to operate. Certification and accreditation is the requirement that agency management officials formally authorize their information systems to process information, thereby accepting the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan. The accreditation decision results in (1) a full authorization to operate,[17] (2) an interim authorization to operate,[18] or (3) no authorization to operate. DOD instructions[19] and DLA's agency handbook provides guidance on the certification and accreditation process.

[17]A full authorization to operate means a system has been properly certified and accredited and any significant vulnerability identified either has been or is actively in the process of being effectively mitigated.

[18]An interim authorization to operate provides a limited authorization to operate the information system under specific terms and conditions and acknowledges greater risk to the agency for a specified, limited time.

[19]DOD Instruction 5200.40, *DOD Information Technology Security Certification and Accreditation Process (*December 30, 1997); DOD 8510.1-M, *DOD Information Technology Security Certification and Accreditation Process Application Manual (*July 31, 2000); and DOD Instruction 8500.1, *Information Assurance (*October 24, 2002).

According to DLA officials, the agency has implemented the practice of issuing authorization to operate decisions on a "time-limited" basis—regardless if certification tasks have been completed because of concern that OMB might not support funding for systems that received an interim authorization to operate decision. However, OMB, DOD, and DLA policies and procedures do not allow for the practice of issuing "time-limited" authorizations; they require interim authorization to operate decisions when all certification tasks have not been completed. To illustrate, the designated approving authority for one of the ten systems we reviewed changed the system's status from an interim authorization to operate to a "time-limited" authorization to operate even though several action items for such authorization had not been met, and this type of authorization is not allowed under current guidance. For example, information assurance personnel had not updated the security plan or completed a risk assessment. Unless DLA complies with the requirements for issuing accreditation decisions, it will not have assurance that its information systems are operating as intended and meeting security requirements.

In addition, DLA did not effectively implement controls to verify the completion of certification tasks. As designed and implemented, DLA divides the responsibilities of the system certifier among the information assurance personnel at its locations and a central review team within the information assurance program office. To help ensure quality over the certification process, the central review team established a DLA quality review checklist to verify the certification tasks performed by the information assurance personnel. However, under the current process, the central review team did not interview information assurance personnel at the locations or conduct on-site visits to verify that certification tasks were performed. Instead, the central review team relies on documentation submitted to them by the information assurance personnel who performed the certification tasks. However, this documentation was not always adequate. For example, the checklist contained questions about whether physical access controls were adequate to protect all facilities housing user workstations, but for the central review team to verify such a task, either an on-site inspection or a diagram of the facility or other documentation to demonstrate the physical access controls in place would have been needed. As a result, the certification process may not provide the authorizing official with objective or sufficient information that is necessary to make credible, risk-based decisions on whether to place an information system into operation.

Improvements Are Needed in Managing and Overseeing the Security Program

Key underlying reasons for the weaknesses in DLA's information security program were that the responsibilities of information assurance managers and information assurance officers were not consistently understood or communicated across the 10 DLA locations we reviewed and the information assurance program office did not maintain the accuracy and completeness of the data contained in the agency's primary reporting tool for managing and overseeing the agencywide information security program. The information assurance program office—as the agency's central security management group for managing and overseeing the security program—is responsible for providing overall security policy and guidance, along with oversight to ensure information assurance managers and information assurance officers adequately perform or execute required information security activities such as those related to performing risk assessments, satisfying security training requirements, testing and evaluating the effectiveness of controls, documenting and reporting plans of action and milestones, and certifying and accrediting systems.

Although the information assurance program office developed information security policies and procedures, it did not maintain them to ensure information assurance personnel had current and sufficient documentation to carry out their responsibilities. For example, of the 17 information assurance managers and information assurance officers at the 10 locations we reviewed:

- nine were unaware of the requirement for security training specific to an employee's information security responsibilities; and
- three were unaware of the requirement to perform annual self assessments, while ten others had varying understandings of how this requirement was to be met.

In addition, data on key information security activities contained in the primary reporting tool were inaccurate or incomplete. For example,

- for a year, the information assurance program office had not entered weaknesses that had been identified during information assurance program reviews into the primary reporting tool;
- information assurance personnel at DLA locations used personal discretion for determining whether or not to report a system deficiency to the information assurance program office for entry and compilation

in the primary reporting tool, thereby potentially underreporting agency level plans of action and milestones; and

- information assurance personnel at both headquarters and the DLA locations did not consistently enter key performance metrics related to plans of action and milestones and security training, thereby potentially underreporting important information used to gauge the health of the security program.

A key reason for these weaknesses was that DLA had no documentation on the system design or its intended use and, therefore, had no instructional material to guide users. As a result, the data in the primary reporting tool were not reliable or effective for reporting metrics to DOD and OMB for FISMA evaluation reporting. Moreover, because the key information had not been entered into the database, the agency did not readily have all the information about the deficiencies of its program and, therefore, did not have complete information about the security posture of its program.

DLA senior officials recognize that the agency's primary reporting tool has not been effectively implemented and used to manage and oversee the security program. Therefore, the agency developed an ad hoc process of data calls to the DLA locations to aggregate the performance data. However, continuation of this ad hoc process will likely not provide the reliable data needed to consistently satisfy FISMA reporting requirements. Until agencywide policies and procedures are sufficiently documented and implemented and are consistently understood and used across the agency, DLA's ability to protect the information and information systems that support its mission will be limited.

Conclusions

DLA has not fully implemented its agencywide information security program, thereby jeopardizing the confidentiality, integrity, and availability of the information and information systems that it relies on to accomplish its mission. Specifically, DLA has not consistently implemented important information security practices and controls, including consistently assessing risk; ensuring that training is provided for employees who have significant responsibilities for information security, and that security training plans are updated and maintained; annually testing and evaluating the effectiveness of management, operational and technical controls; documenting and reporting complete plans of action and milestones; implementing a fully effective certification and accreditation process; and maintaining the accuracy and completeness of the data contained in the

primary reporting tool. Although DLA's efforts in developing and implementing its information security program have merit, it has not taken all the necessary steps to ensure the security of the information and information systems that support its operations. Ensuring that the agency implements key information security practices and controls requires top management support and leadership and consistent and effective management oversight and monitoring. Until DLA takes steps to address these weaknesses and fully implements its information security program, it will have limited assurance that agency operations and assets are adequately protected.

Recommendations for Executive Actions

To assist DLA in fully implementing its information security program, we are making recommendations to the Secretary of Defense to direct the DLA Director to implement key information security practices and controls by:

- consistently assessing risks that could result from the unauthorized access, use, disclosure or destruction of information and information;
- ensuring that training is provided for employees who have significant responsibilities for information security;
- ensuring that security training plans are updated and maintained;
- ensuring appropriate monitoring of the agency's security training program;
- ensuring that annual security test and evaluation activities include management, operational, and technical controls of every information system in DLA's inventory;
- documenting and reporting complete plans of action and milestones;
- establishing specific guidance or instructions to information assurance managers and information assurance officers on what—or how—to document and report plans of action and milestones for system deficiencies;
- discontinuing the practice of issuing "time-limited" authorization to operate accreditation decisions when certification tasks have not been completed;

- ensuring that the DLA central review team verifies that certification tasks have been completed; and

- maintaining the accuracy and completeness of the data contained in the agency's primary reporting tool for recording, tracking, and reporting performance metrics on information security practices and controls.

Agency Comments and Our Evaluation

In providing written comments on a draft of this report (reprinted in app. II), the Deputy Under Secretary of Defense (Business Transformation) concurred with most of our recommendations and described ongoing and planned efforts to address them. Specifically, he stated that DLA has taken several actions to fully implement an effective agencywide information security program, including publishing a DOD manual that will soon be released to provide detailed guidance on training for employees who have significant information security responsibility. He also stated that DLA is issuing an interim mandatory guide that will soon be released to assist users in documenting and preparing plans of action and milestones, and reinforcing policy requirements for making accreditation decisions.

The Deputy Under Secretary of Defense disagreed with our draft recommendation to ensure the testing and evaluation of the effectiveness of security controls for all systems annually. He stated that this recommendation would require all information assurance controls for all systems be tested and evaluated every year, which essentially amounts to annual recertification. The department further stated that the level of test and evaluation is neither practical nor cost-effective and that the combination of DLA's assessments, tests, and reviews allow them to ensure compliance of their controls in accordance with DOD Instruction 8500.2.

The intent of our draft recommendation was not to require that *all* information assurance controls for all systems be tested and evaluated annually. Rather, the intent of our draft recommendation, consistent with FISMA requirements, was to ensure that DLA's annual security test and evaluation activities *include* management, operational, and technical controls of every information system in its inventory. As stated in our report, while DLA generally assessed technical controls annually of every system in its inventory, it did not annually test and evaluate management and operational controls of those systems. We agree that testing and evaluating all controls for every system annually may not be cost-effective. However, unless DLA's annual testing and evaluation activities include management and operational controls, as well as the technical controls of

its systems, it may not be able to ensure the confidentiality, integrity, and availability of its information and information systems. Accordingly, we have clarified our recommendation to state that the Secretary of Defense direct the DLA Director to ensure that annual security test and evaluation activities include management, operational, and technical controls of every information system in DLA's inventory.

The Deputy Under Secretary of Defense also disagreed with our draft recommendation to document procedures for performing certification responsibilities that include specific responsibilities related to using the checklist. He stated that the Secretary of Defense provided sufficient direction to agency directors on the certification and accreditation process through DOD Instruction 5200.40, and that additional guidelines on the certification and accreditation process are provided in DOD 8510.1-M. He further stated that DOD 8510.1-M contains a "minimum activities checklist" that all DOD Components are expected to follow when conducting certifications and that DLA's information assurance One Book policy includes roles and responsibilities for performing security certification and accreditation.

Our draft recommendation refers to the DLA quality review checklist used by the agency's central review team to verify completion of certification tasks, not to the DOD "minimum activities checklist" described in DOD 8510.1-M. Unless certification tasks performed by information assurance personnel at the various DLA locations have been verified, the authorizing official may not have objective or sufficient information that is necessary to make credible, risk-based decisions on whether to place an information system into operation. Accordingly, we have clarified our recommendation to state that the Secretary of Defense direct the DLA Director to ensure that the DLA central review team verifies that certification tasks have been completed.

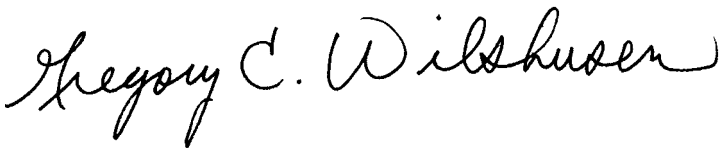
The Deputy Under Secretary of Defense also disagreed with our draft recommendation to update and maintain the agency's primary reporting tool for recording, tracking, and reporting performance metrics on information security practices and controls. He stated that the primary reporting tool was developed and maintained by DLA and that responsibility for updating and sustaining the tool was transferred to an internal application development team for continued maintenance and support. He also stated that DLA initiated implementation of enterprise standard DOD solutions that will replace the functionality currently

provided by the agency reporting tool and that sustainment of the tool would not be cost effective or efficient.

The intent of our draft recommendation was to update and maintain the accuracy and completeness of data entered into DLA's primary reporting tool, not the application programs. While DLA has several initiatives underway at various stages of development and implementation that are intended to introduce new functionality or replace some of the existing functionality in the agency reporting tool, none of these initiatives have been fully implemented throughout the agency. If DLA continues to use a tool for managing and overseeing its information assurance program, the fundamental practice of having accurate and complete data—whether in the current tool or in a future tool—is important to ensure the data are reliable for reporting performance metrics on key information security practices and controls to DOD and OMB for FISMA evaluation reporting. Accordingly, we have clarified our recommendation to state that the Secretary of Defense direct the DLA Director to maintain the accuracy and completeness of the data contained in the agency's primary reporting tool for recording, tracking, and reporting performance metrics on information security practices and controls.

We are sending copies of this report to the Deputy Under Secretary of Defense (Business Transformation); Assistant Secretary of Defense, Networks and Information Integration; DLA Director; officials within DLA's Information Operations and Information Assurance office; and the Acting DOD Inspector General. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions regarding this report, please contact me at (202) 512-6244 or by e-mail at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues

Scope and Methodology

To determine whether the Defense Logistics Agency (DLA) had implemented an effective agencywide information security program, we reviewed the Department of Defense (DOD) and agencywide information security policies, directives, instructions, and handbooks. We also evaluated DLA's agencywide tool—the Comprehensive Information Assurance Knowledgebase—for aggregating the agency's performance data on information security activities that are required by the Federal Information Security Management Act of 2002 (FISMA), such as the number and percentage of risk assessments performed, employees with significant information security responsibilities that received training to perform their duties, and weaknesses for which the agency had plans of action and milestones. To gain insight into DLA's certification and accreditation process, we reviewed the agency's methods and practices for identifying vulnerabilities and risks and the process for certifying systems and making accreditation decisions. We assessed whether DLA's information security program was consistent with relevant DOD policies and procedures, as well as with the requirements of FISMA, applicable Office of Management and Budget (OMB) policies,[1] and National Institute of Standards and Technology (NIST) guidance.

We also assessed whether selected information security plans and documents related to risk assessments, testing and evaluation, and plans of action and milestones were current and complete. To accomplish this, we non-randomly selected 10 sensitive but unclassified systems.[2] The 10 systems came from 10 different DLA locations and included 3 systems, 4 sites, and 3 types.[3] We selected these systems to maximize variety in criticality and geographic locations. We also conducted telephone interviews with 17 information assurance managers and information assurance officers from the 10 locations in order to gain insight into their understanding of FISMA requirements, relevant OMB policies, NIST guidance, and agencywide and DOD policies and procedures.

[1]Office of Management and Budget, Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (Washington, D.C.: Nov. 28, 2000).

[2]The system security authorization agreement is a single source data package for all information pertaining to the certification and accreditation of a particular site or system to, among other things, guide actions, document decisions, specify information security requirements, and maintain operational systems security.

[3]A type system security authorization agreement is developed when an information system has been replicated with the same configuration and has been deployed at multiple locations.

We performed our review at DLA Headquarters, located at Ft. Belvoir, Virginia; DLA Supply Center, located at Columbus, Ohio; and DLA's Business Processing Center, located at Denver, Colorado, from September 2004 to July 2005, in accordance with generally accepted government auditing standards.

Comments from the Department of Defense

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

SEP 21 2005

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Wilshusen:

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-05-901, INFORMATION SECURITY: The Defense Logistics Agency Need to Fully Implement Its Security Program, dated August 19, 2005, (GAO Code 310542).

The Department has DoD instructions that comply with four of the ten recommendations and is preparing to issue detailed interim mandatory guidance for three additional recommendations. However, we non-concur with the remaining three recommendations. Our response to all ten GAO recommendations is enclosed.

We appreciate the opportunity to provide comments on the draft report and look forward to on-going engagement and discussion with the GAO in the area of Information Security.

Sincerely,

Paul Brinkley
Deputy Under Secretary of Defense,
(Business Transformation)

Enclosure:
As Stated

GAO DRAFT REPORT - DATED AUGUST 19, 2005
GAO CODE 310542/GAO-05-901

"INFORMATION SECURITY: THE DEFENSE LOGISTICS AGENCY NEEDS TO FULLY IMPLEMENT ITS SECURITY PROGRAM"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommended that the Secretary of Defense direct the DLA Director to implement key information security practices and controls by: consistently assessing risks that could result from the unauthorized access, use, disclosure or destruction of information and information. (p. 21/GAO Draft Report)

DOD RESPONSE: Concur. Department of Defense Instruction (DoDI) 8500.2 directs all services and agencies to assess risks that could result from the unauthorized access, use, disclosure or destruction of information and information. Experience has shown that identifying specific threats to individual information systems can be a difficult, expensive, time consuming task that often ultimately relies on subjective judgment. DoDI 8500.2 uses the baseline sets of IA Controls to mitigate risk based on the value of the information protected. This value is as expressed in terms of Mission Assurance Category (MAC) for availability and integrity capabilities Confidentiality Level for classification, sensitivity, or need-to-know. Essentially, as DoD assigns greater value to information (i.e., gives it a higher MAC or Confidentiality Level) it protects against a greater assumed threat. This is accomplished both by increasing the number of IA Controls and, in appropriate cases, making the IA Controls more stringent as the value of the information increases. This is not to say that Designated Accrediting/Approving Authority (DAA) shouldn't be concerned about special threat considerations but, as a general rule, if the IA Controls for a particular MAC and confidentiality Level are properly applied and tested, the system is adequately protected.

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense direct the DLA Director to implement key information security practices and controls by: ensuring that training is provided for employees who have significant responsibilities for information security. (p. 21/GAO Draft Report)

DOD RESPONSE: Concur. DoD Directive 8570.1, Information Assurance (IA) Training, Certification, and Workforce Management released in August 2004 directs training for all DoD affiliated individuals with significant IA responsibilities. Draft DoD 8570.1-M, the manual that provides detailed implementation guidance for IA training, is in the final stage of coordination and will be released soon. Additionally, the Director, DLA reports that in May 2004, the DLA Chief Information Officer (CIO) was briefed on weaknesses in the area of IA skills and qualifications. Prior to GAO's completion of this report the DLA IA Program Office took steps to develop a Comprehensive IA Training Program plan to include a work

breakdown structure for IA functions, IA tasks and skills qualification requirements, identification of sources to provide DoD IA training requirements, and training metrics. DLA recognized weaknesses and deficiencies in the area of IA training and took proactive steps to address this problem. Copies of the afore-mentioned briefing and Statement of Work regarding the IA training program were provided to GAO.

RECOMMENDATION 3: The GAO recommended that the Secretary of Defense direct the DLA Director to implement key information security practices and controls by: ensuring that security training plans are updated and maintained. (p. 22/GAO Draft Report)

DOD RESPONSE: Concur. See response to Recommendation #2, above.

RECOMMENDATION 4: The GAO recommended that the Secretary of Defense direct the DLA Director to implement key information security practices and controls by: having a dedicated individual responsible for monitoring the agency's security training program. (p. 22/GAO Draft Report)

DOD RESPONSE: Concur. DoD Directive 8500.1, "Information Assurance," October 24, 2002 requires that the Heads of DoD Components ensure that IA awareness, training, education, and professionalization are provided to all Component personnel commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DoD information systems. DoD Directive 8570.1 reinforces this guidance and DoD 8570.1-M will provide detailed guidance on agencies' IA training programs.

RECOMMENDATION 5: The GAO recommended that the Secretary of Defense direct the DLA Director to implement key information security practices and controls by: ensuring the testing and evaluating of the effectiveness of security controls for all systems annually. (p. 22/GAO Draft Report)

DOD RESPONSE: Non-Concur. This recommendation would require all IA controls for all systems be tested and evaluated every year, which essentially amounts to annual recertification. The burden associated with this level of test and evaluation is neither practical nor cost effective. DLA's strategy for ensuring compliance with DoD IA controls meet the requirements stipulated in E3.3.10 of DODI 8500.2 by requiring a combination of self-assessments, independent assessments and audits, formal testing and certification activities, host and network vulnerability or penetration testing, and IA program reviews. We believe this strategy is sufficient to achieve appropriate test and evaluation of security controls.

RECOMMENDATION 6: The GAO recommended that the Secretary of Defense direct the DLA Director to implement key information security practices and controls: by documenting and reporting complete plans of action and milestones. (p. 22/GAO Draft Report)

DOD RESPONSE: Concur. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD NII/DoD CIO) is finalizing for issuance, detailed interim mandatory guidance on the preparation and submission of Plans of Actions and Milestones (POA&M). That guidance will subsequently be incorporated into permanent DoD policies, as appropriate. The DLA One Book currently requires POA&M as part of the DLA security certification effort and will be modified as necessary to comply with the new DoD policy when it is issued.

RECOMMENDATION 7: The GAO recommended that the Secretary of Defense direct the DLA Director to implement key information security practices and controls by: establishing specific guidance or instructions to information assurance officers on what or how to document and report plans of action and milestones for system deficiencies. (p. 22/GAO Draft Report)

DOD RESPONSE: Concur. See response to Recommendation # 6, above.

RECOMMENDATION 8: The GAO recommended that the Secretary of Defense direct the DLA Director to implement key information security practices and controls by: discontinuing the practice of issuing "time-limited" authorization to operate accreditation decision. (p. 22/GAO Draft Report)

DOD RESPONSE: Concur. The interim POA&M guidance discussed in the response to Recommendation #6 above establishes criteria that preclude issuance of a "time limited" ATO when an IATO is appropriate. This policy direction will be reinforced by a new DoD instruction on certification and accreditation that will be issued this calendar year

RECOMMENDATION 9: The GAO recommended that the Secretary of Defense direct the DLA Director to implement key information security practices and controls by: documenting procedures for performing certification responsibilities that include specific responsibilities related to using the checklist. (p. 22/GAO Draft Report)

DOD RESPONSE: Non-Concur. The Secretary of Defense provided sufficient direction to Agency Directors through Department of Defense Instruction (DoDI) 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997. This directive establishes the basis for performing security certification and accreditation throughout the Department of Defense. Additional guidelines on the process are provided in DoD 8510.1-M, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 2000. The manual does contain a minimum activities checklist that all DoD Components are expected to follow when conducting certifications. Agency Directors have managerial latitude to ensure compliance with DoD issued Policy. DLA IA Management and Operational Control One Book Chapters

do include roles and responsibilities for performing security certification and accreditation in accordance with above references.

RECOMMENDATION 10: The GAO recommended that the Secretary of Defense direct the DLA Director to implement key information security practices and controls by: updating and maintaining the agency's primary reporting tool for recording, tracking, and reporting performance metrics on information security practices and controls.
(p. 22/GAO Draft Report)

DOD RESPONSE: Non-Concur. The Agency's current reporting tool, CIAK, is a Government Off the Shelf (GOTS) capability developed and maintained by DLA. Prior to this Audit, responsibility for update and sustainment of the CIAK tool was transferred to an internal application development team for upgrade to facilitate continued supportability of this locally developed tool. In the interim DLA initiated implementation of enterprise standard DoD solutions (i.e., Vulnerability Management System, eMASS, eRetina, and Hercules) that will replace the functionality currently provided by CIAK. Sustainment of a GOTS tool is not considered cost effective or efficient. GAO was briefed on the status of these initiatives.

GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen (202) 512-6244

Staff Acknowledgments

In addition to the individual named above, Jenniffer Wilson, Assistant Director, Barbara Collier, Joanne Fiorino, Sharon Kittrell, Frank Maguire, John Ortiz, and Chuck Roney made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER