United States Government Accountability Office

GAO

Report to the Ranking Member, Committee on Oversight and Government Reform, House of Representatives

August 2007

INFORMATION SECURITY

Selected Departments Need to Address Challenges in Implementing Statutory Requirements

GAO

Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-528, a report to the Ranking Member, Committee on Oversight and Government Reform, House of Representatives

August 2007

INFORMATION SECURITY

Selected Departments Need to Address Challenges in Implementing Statutory Requirements

Why GAO Did This Study

The Federal Information Security Management Act of 2002 (FISMA) strengthened security requirements by, among other things, requiring federal agencies to establish programs to provide cost-effective security for information and information systems. In overseeing FISMA implementation, the Office of Management and Budget (OMB) has established supporting processes and reporting requirements. However, 4 years into implementation of the act, agencies have not yet fully implemented key provisions.

In this context, GAO determined what challenges or obstacles inhibit the implementation of the information security provisions of FISMA at the Departments of Defense, Homeland Security, Justice, and State. To do this, GAO reviewed and analyzed department policies, procedures, and reports related to department information security programs and interviewed agency officials.

What GAO Recommends

GAO is making recommendations to assist the four departments in addressing the challenges they face in implementing FISMA requirements for information security programs. Homeland Security, Justice, and State generally agreed with the recommendations. However, Defense did not agree with three of GAO's six recommendations. GAO continues to stand by its recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-528.

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

Defense, Homeland Security, Justice, and State face challenges in implementing key information security control activities required by FISMA and by OMB in its oversight role. These activities include

- creating and maintaining an inventory of major systems,
- implementing common security configurations,
- ensuring that staff receive information security training,
- testing and evaluating controls,
- taking remedial actions where deficiencies are found, and
- certifying and accrediting systems for operation.

As shown in the table below, the four departments were challenged in several of these areas. For example, Defense is challenged in developing a complete FISMA inventory of systems because it has different definitions of what constitutes a "system." As another example, Homeland Security reported that the tool it uses to report security training counts each course taken, instead of tracking that an individual has taken a specialized course. As a result, the department lacks assurance that all users have received appropriate training. Until the departments address their challenges and fully implement effective departmentwide information security programs, increased risk exists that they will not be able to effectively protect the confidentiality, integrity, and availability of their information and information systems.

Security Requirements That Challenge Selected Departments

Requirement	Defense	Homeland Security	Justice	State
Inventory of major systems	X			X
Enforcing system configuration policies	X	X	X	
Information security training	X	X		X
Testing and evaluation of controls	X	X	X	X
Remedial actions	X	X	X	X
Certification and accreditation of systems	X	X		X

Source: GAO.

Contents

Tables

Figure

Abbreviations

CIO	chief information officer
FISMA	Federal Information Security Management Act of 2002
IG	inspectors general
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

August 31, 2007

The Honorable Tom Davis
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Dear Mr. Davis:

The Federal Information Security Management Act of 2002 (FISMA) strengthened security requirements by, among other things, requiring departments to establish agencywide programs to provide cost-effective security for information and information systems. Information security is a critical consideration for any organization that depends on information systems and networks to carry out its mission or business. It is especially important for federal departments where maintaining the public trust is essential.

In this context, our objective in this report was to determine the challenges or obstacles that inhibit the implementation of the information security provisions of FISMA at the Departments of Defense, Homeland Security, Justice, and State. To achieve our objective, we analyzed various department policies and procedures and examined agency and inspectors general (IG) reports related to their information security programs. We also interviewed information security program officials from each department and selected component agencies of the departments.

We performed our work in Washington, D.C., from July 2006 through May 2007 in accordance with generally accepted government auditing standards. See appendix I for additional details on our objective, scope, and methodology.

Results in Brief

Defense, Homeland Security, Justice, and State face challenges in implementing key information security control activities required by FISMA and the Office of Management and Budget (OMB) to establish an effective departmentwide information security program. These activities include creating and maintaining an inventory of major systems, implementing common security configurations, ensuring that staff receives information security training, testing and evaluating controls, taking remedial actions where deficiencies are found, and certifying and accrediting systems for operation.

The challenges in implementing these FISMA activities at the four departments include the following:

- Defense and State do not have complete and accurate system inventories as verified by their IGs.

- Although each of the four departments has established a departmentwide policy for common security configurations, only State reported successfully implementing its security configurations for all system platforms.

- None of the four departments has trained all of its personnel as required by FISMA.

- Although these departments reported progress in the percentage of systems in which security controls were tested, guidance for developing plans of action and milestones to address deficiencies uncovered by testing was not sufficient, and processes were not established to carry out such plans consistently. In addition, components of Defense, Homeland Security, and State show wide variations in their reported accomplishment of security controls testing.

- Of the four departments, only Justice has achieved full certification and accreditation of its information systems.

The reasons for these challenges vary. For example, Defense is challenged in developing a complete FISMA inventory of systems because its components have different definitions of what constitutes a "system." As another example, Homeland Security reported that the tool it uses to report training counts each course taken, instead of tracking that an individual has taken a specialized course. As a result, the department lacks assurance that all users have received appropriate training. Until the departments address their challenges and fully implement effective departmentwide information security programs, they may not be able to effectively protect the confidentiality, integrity, and availability of their information and information systems.

We are making recommendations to the Secretaries of Defense, Homeland Security, and State, as well as the U.S. Attorney General, to assist these departments in addressing the challenges in six areas, including agency information security training programs and department-level remediation processes.

We obtained written comments on a draft of this report from Defense, Homeland Security, Justice, and State; these comments are reproduced in appendixes II to V, respectively. Homeland Security, Justice, and State generally agreed with all recommendations. Defense generally agreed with two of our recommendations and partially concurred with one, but it disagreed with the remaining three recommendations. Specifically, Defense did not agree with our recommendation to develop and implement a departmentwide definition of a major information system that is accepted by the Defense IG. Defense said that it already has a standard definition for FISMA reporting. However, although Defense does have such a definition, its own guidance, as we discuss in our report, provides at least two definitions of a system. This forces the components, and the Defense IG, to make independent interpretations of what should be included in the inventory for FISMA reporting purposes, leading to inconsistent results. In addition, Defense did not agree with our recommendation to complete the development of the departmentwide remediation process and finalize the remediation guidance; however, Defense commented that the interim guidance, discussed in our report, will be finalized in September 2007. Lastly, Defense did not agree with our recommendation to ensure that all information systems receive a full authorization to operate and to improve the department's certification and accreditation process. Although interim authorizations to operate represent some level of accepting risk, we believe that without a full authorization to operate there is an increased risk to the department's operations. We continue to believe that all of our recommendations have merit.

In addition, Defense and State commented that the report findings did not fully illustrate their perspective on implementing FISMA activities, such as the department's efforts and progress, or external challenges. Throughout our report, where appropriate, we acknowledge the progress made by the departments; however, each continues to face individual challenges to implementing an effective and robust information security program.

Background

Federal agencies rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Protecting federal computer systems and the systems that support critical infrastructures has never been more important, owing to 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. Without proper safeguards, there is enormous 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.

Federal Law and Policy Establish Federal Information Security Requirements

Enacted into law on December 17, 2002, as Title III of the E-Government Act of 2002, FISMA authorized and strengthened information security program, evaluation, and reporting requirements. It assigns specific responsibilities to agency heads, chief information officers (CIO), and IGs. It also assigns OMB and the National Institute of Standards and Technology (NIST) with responsibilities with regard to oversight and guidance. Among other things, OMB is responsible for overseeing agency information security policies and practices, including developing and overseeing guidance on information security and overseeing compliance. NIST is tasked with developing standards and guidance for implementation of FISMA requirements by federal agencies. However, 4 years into the implementation of FISMA, many agencies continue to exhibit weaknesses in carrying out the act’s requirements.

Overall, FISMA requires each agency to develop, document, and implement an agencywide information security program. This program should provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Among the key activities and responsibilities associated with implementing this program are the following:

- Development, maintenance, and annual update of an inventory of major information systems (including major national security systems) that are operated by the agency or are under its control.
- Risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system, including through compliance with minimally acceptable system configuration requirements.

- Security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency, and training for personnel with significant responsibilities for information security.

- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but not less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems.

- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.

In addition, as part of its responsibilities for overseeing the establishment of agency information security programs in accordance with FISMA, OMB requires that systems be certified and accredited, a process by which senior agency officials certify that the risk level of information systems is acceptable and that the systems are approved for operation.

Because these key activities are interdependent, weaknesses in one activity challenge the effective accomplishment of other FISMA activities. For example, a complete and accurate system inventory provides a basis for tracking FISMA compliance and for testing the effectiveness of security controls for all systems and their components—necessary to assess system risk. The inventory and risk assessments in turn feed an agency's strategy for managing risk and maintaining departmental risk-based policies and procedures. Similarly, effectively training personnel strengthens an agency's ability to properly and consistently implement required security controls and to maintain an effective program over time.

To help ensure that agencies are accountable for meeting the act's requirements, FISMA requires each agency to annually report to OMB, selected congressional committees, and the Comptroller General of the United States on the adequacy of information security policies, procedures, and practices and on compliance with requirements. Agency heads are required to annually report the results of their independent evaluations to OMB.

Departments Face Challenges in Implementing FISMA Requirements

Defense, Homeland Security, Justice, and State face challenges in implementing key information security control activities required by FISMA and OMB, as shown in table 1.

Table 1: Security Requirements That Challenge Selected Departments

Requirement	Defense	Homeland Security	Justice	State
Inventory of major systems	X			X
Enforcing system configuration policies	X	X	X	
Information security training	X	X		X
Testing and evaluation of controls	X	X	X	X
Remedial actions	X	X	X	X
Certification and accreditation of systems	X	X		X

Source: GAO.

The reasons that the departments are challenged in these areas vary. For example, some departments attribute weaknesses to limitations in the tools and processes they use to perform certain activities (such as training and remedial actions). Until the departments address these challenges and fully implement an effective departmentwide information security program, they increase the risk that they may not effectively protect the confidentiality, integrity, and availability of their information and information systems.

Identifying an Inventory of Major Information Systems Presents a Challenge for Two of the Four Departments

FISMA and OMB guidance require each agency to develop, maintain, and annually update an inventory of major information systems[1] that are operated by the department or that are under its control. For each system, OMB requires agencies to use their inventories to support information resource management, including monitoring, testing, and evaluation of information security controls.

Of the four departments, Homeland Security and Justice reported having complete system inventories. OMB has announced in its *FY 2006 Report to Congress on Implementation of The Federal Information Security*

[1] OMB Circular A-130, *Management of Federal Information Resources* (Washington, D.C.: November 2000), defines the term "major information system" as an information system that requires special management attention because of its importance to a department mission; its high development, operating, or maintenance costs; or its significant role in the administration of department programs, finances, property, or other resources.

Management Act of 2002 that Justice's automated tool will be available to other federal agencies under the information system security line of business. However, Defense and State have not developed accurate and complete FISMA inventories.

Since 2004, the IG at Defense has reported that the department does not have a complete and accurate inventory of its major information systems. A contributing factor to this incomplete inventory is that Defense does not have a common definition of an information system. As noted in guidance that the department issued in 2006, Defense policies have at least two definitions of a system, neither of which provides consistent criteria for what should be entered into a FISMA inventory.[2] The 2006 guidance provides a third set of criteria and states that the two policy definitions should act only as a starting point. However, Defense components must make independent interpretations of whether the asset under evaluation should be reported as a system for FISMA purposes, and the varied interpretations create discrepancies in the inventory. For example, Department of the Navy officials stated that not having a common definition of what is an information technology (IT) system makes it virtually impossible to distinguish between a system and its constituent subsystems/applications versus a family of systems and constituent systems. Without establishing and enforcing the use of one common definition, Defense cannot implement consistent inventory management practices across its components.

State has developed a definition of a major information system for the purposes of its inventory; however, there is disagreement with its IG regarding how to apply the definition to individual IT assets—either separately or as part of a consolidated system. In 2006, State's IG found Web applications that State officials had not included separately in their FISMA inventory. Because of time limitations, the IG was unable to determine whether other IT assets were missing from the inventory and rejected the entire FISMA inventory maintained by State. State now has an effort under way to resolve this challenge and identify all Web applications for inclusion in the inventory. If this effort results in agreement with State's IG, it could help the department in obtaining independent verification of its system inventory.

[2] Memorandum from the Chief Information Officer, *Department of Defense (DOD) Information Technology (IT) Portfolio Repository (DITPR) and DOD SIPRNet IT Registry Annual Guidance for 2006* (May 17, 2006).

Three of the Four Departments Are Challenged in Implementing Common Security Configurations for All Systems

FISMA requires that agency information security programs include risk-based policies and procedures that ensure that information security is addressed throughout the life cycle of each information system, including through compliance with minimally acceptable system configuration requirements. According to the NIST guidance for implementing configuration management requirements, the policies for baseline system configurations provide information about the makeup of a particular system component (e.g., the standard software load for a workstation or notebook computer, including updated patch information). In addition, the system configuration settings are the adjustable parameters of these components that enforce the agency security policy consistent with operational requirements.[3]

According to the fiscal year 2006 CIO FISMA reports, all four departments reported that they had established a departmentwide policy for common security configurations. However, as detailed in table 2, only State reported successfully implementing its common configuration policy on all system platforms. State attributes its success to the development and implementation of a strong configuration management compliance program known as "Evaluation and Verification." According to State, the program conducts remote scans to confirm whether State systems are operating as intended, in accordance with mandatory security configuration requirements. The program also helps provide the CIO with an additional level of assurance by identifying known security vulnerabilities within State systems and applications. However, Defense, Homeland Security, and Justice reported inconsistent implementation of common secure configuration policies across departmental systems.

Table 2: Weaknesses in Implementation of Common Security Configurations for Fiscal Year 2006

Product	Defense	Homeland Security	Justice	State
Windows XP Professional				
Windows NT	X	X	X	
Windows 2000 Professional		X		
Windows 2000 Server		X	X	
Windows 2003 Server				

[3] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, as amended (Washington, D.C.: December 2006).

Product	Defense	Homeland Security	Justice	State
Solaris				N/A
HP-UX	X	X	X	N/A
Linux	X	X		
Cisco Router IOS				
Oracle		X	X	

Legend:

X = Agency reported that 95 percent or fewer of the systems running this software are in compliance with its configuration policy; empty cells indicate that the agency was compliant with the configuration policy for 96 to 100 percent of the systems running this software.

N/A = Agency does not operate this software.

Source: Agency CIO FISMA reports for fiscal year 2006.

Without consistent implementation of common security configurations across systems, these departments increase the risk that their systems will have avoidable security vulnerabilities.

Three Departments Face Challenges in Identifying Personnel Needing Training

FISMA mandates that all federal employees and contractors who use department information systems be provided with periodic training in information security awareness and accepted information security practices. FISMA also requires agencies to provide appropriate training on information security to personnel who have significant security responsibilities. This training, described in NIST guidance,[4] should inform personnel, including contractors and other users of information systems supporting the operations and assets of an agency, of information security risks associated with their activities and of the roles and responsibilities of personnel to properly and effectively implement the controls required by policies and procedures that are designed to reduce these risks.

Although the four departments reported that they have implemented training for the majority of their personnel, three departments face individual challenges, as follows:

- Defense officials reported that the department's components have not been able to document and track whether their 2.3 million users (who are

[4] NIST Special Publications 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (Gaithersburg, Md.: April 1998), and 800-50, *Building an Information Technology Security Awareness and Training Program* (Gaithersburg, Md.: October 2003).

distributed worldwide) have received the required awareness training. For example, the Department of the Army is currently unable to ensure that users who access its IT systems have taken the required awareness training. To overcome this obstacle, the Army has identified a need for a componentwide tool that will ensure that only users who have taken the required training are permitted to access its systems. In addition, Defense officials stated that several of its components have difficulty in identifying and tracking all employees who have significant IT security responsibilities. For example, U.S. Air Force officials stated that it is challenging to identify these personnel when they are not within an IT functional area, and the Defense Information Systems Agency stated that it is difficult to track information security training requirements for contractors because of the lack of a central personnel database. In fiscal year 2006, Defense issued a training and workforce improvement manual to provide instructions to components to account for and track training of all IT security personnel, even in the absence of a central personnel database. Such a manual, if properly implemented, could help Defense ensure that all personnel receive appropriate security training. However, until Defense implements a mechanism to track training of personnel, it will be unable to verify that personnel are effectively trained in their information security roles and responsibilities.

- Homeland Security has not been able to ensure that employees who have significant IT security responsibilities receive specialized training. Specifically, the Homeland Security IG reported that the department has not yet established a program to train all individuals who have significant IT security responsibilities. Furthermore, in fiscal year 2006, the IG reported that Homeland Security did not ensure that employees with these responsibilities had completed the required training in the department’s process for validating the annual FISMA metrics. In addition, the department reported that it was unable to accurately report on the percentage of employees who have received specialized training because its reporting tool counts each course taken, instead of tracking that an individual has taken a specialized course. As a result, it could not be assured that all users had completed required training. Homeland Security has efforts under way to implement a centralized Web-based learning management system that will track the completion of security training. Until such a system is properly implemented, the department is unable to identify personnel who have not completed required training.

- State has not been able to verify that all employees and contractors have received required annual awareness training. The State IG reported that the department was unable to determine the total number of users who are required to complete the annual awareness training because of duplicate entries in State's database that generates the number of users. Without adequate controls to ensure the accuracy of training information, the department cannot confirm that all personnel who require awareness training have actually completed the training.

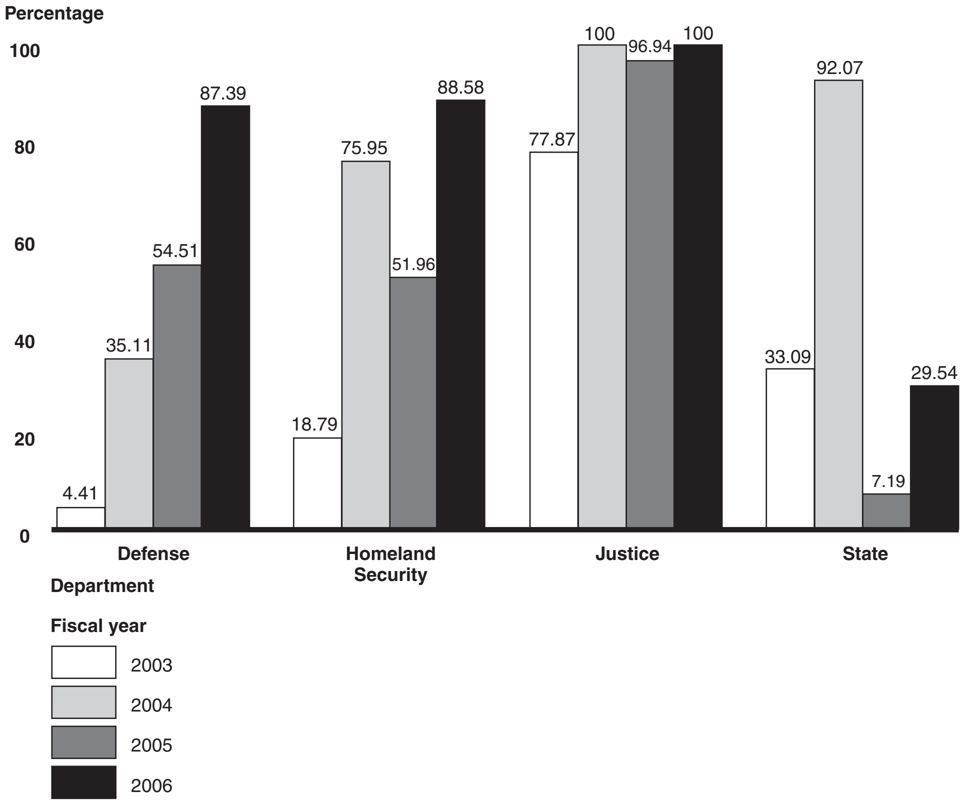
Departments Have Weaknesses in the Testing and Evaluation of Their Information Security Programs

FISMA requires that department information security programs include periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices. This testing is to be performed with a frequency that depends on risk, but no less than annually. It is to include testing of management, operational, and technical controls for every information system identified in the FISMA-required inventory of major systems. Furthermore, a review of each system is essential to determine the program's effectiveness. However, as we explained in a prior report, the depth and breadth of such system reviews are flexible and depend on several factors, such as (1) the potential risk and magnitude of harm to the system or data, (2) the relative comprehensiveness of the last year's review, and (3) the adequacy and successful implementation of the plan of action and milestones for weaknesses in the system.[5]

Each of the four departments reported progress in increasing the percentage of systems for which reviews were performed and security controls tested (see fig. 1).

[5] GAO, *Information Security: Agencies Need to Develop and Implement Adequate Policies for Periodic Testing*, GAO-07-65 (Washington, D.C.: Oct. 20, 2006).

Figure 1: Percentage of Systems for Which Security Controls Have Been Tested and Evaluated in Fiscal Years 2003–2006



Source: GAO analysis of agency-reported data.

However, the departments have not demonstrated adequate and effective monitoring and evaluation of information security controls. In previous work, we showed that guidance for performing such assessments at these departments was not sufficient, and that the departments have not adequately and effectively implemented policies for periodically testing and evaluating information security controls.[6] We reported that the policies for the 24 Chief Financial Officer's Act agencies for periodically testing and evaluating security controls did not fully address elements included in OMB and NIST guidelines and standards for performing effective security testing and evaluations. In particular, we reported that Defense, Homeland Security, Justice, and State had not established

[6] GAO-07-65.

adequate instructions for determining the depth and breadth of periodic tests. Table 3 indicates weaknesses in developing and promulgating documented policies to address the security elements needed for effective testing.

Table 3: Weaknesses in Policies of Selected Departments, by Security Control Testing Element

	Security controls testing element					
Department	Identify the frequency of periodic testing	Define roles and responsibilities	Provide instructions for selecting minimum security controls evaluated during periodic testing	Specify the identification and testing of common security controls	Provide instructions on determining the depth and breath of testing	Describe a process for documenting weaknesses in remediation plans
Defense		X	X	X	X	X
Homeland Security		X		X	X	
Justice			X	X	X	
State	X	X		X	X	

Legend:

X = weakness

Source: GAO analysis of department policies (as of February 2006).

Ensuring that departmental policies are sufficient to address federal standards and guidelines helps to ensure their effective implementation in meeting FISMA requirements for testing and evaluation. Until these departments address the weaknesses in their policies, departments may not be able to overcome the weaknesses in the corresponding security control activities required by FISMA.

In addition, the departments reported that security control testing was not performed consistently across all components in three of the four departments. Justice was the only department to report that all of its components successfully completed the required annual security control and contingency plan testing on all their systems. This success was achieved through the department's efforts to establish and maintain a system inventory and to manage departmentwide risks. In contrast, Defense, Homeland Security, and State reported inconsistent testing of security controls and contingency plans among their components. As shown in tables 4 to 6, components of Defense, Homeland Security, and State reported widely varying percentages of systems tested. For example, at Homeland Security, the percentages for contingency plan testing ranged from 39 to 97 percent.

Table 4: Percentage of Systems Tested by Selected Department of Defense Components

Component	Security control testing	Contingency plan testing
Air Force	82%	79%
Army/Army Corps of Engineers	86	86
Defense Information Systems Agency	93	88
Navy/Marine Corps	91	90

Source: GAO analysis based on 2006 Defense FISMA report data.

Table 5: Percentage of Systems Tested by Selected Homeland Security Components

Component	Security control testing	Contingency plan testing
Coast Guard	98%	45%
Customs and Immigration Service	77	78
Federal Emergency Management Agency	94	68
Immigration and Customs Enforcement	83	39
Transportation Security Administration	94	97

Source: GAO analysis based on 2006 Homeland Security FISMA report data.

Table 6: Percentage of Systems Tested by Selected State Department Bureaus

Component	Security control testing	Contingency plan testing
Diplomatic Security	8%	71%
Information Resource Management	34	72

Source: GAO analysis based on 2006 State FISMA report data.

Without consistent security testing across all components, a department lacks assurance that it is maintaining adequate information security departmentwide.

Departments Have Weaknesses in Processes for Developing Remediation Plans

In addition to periodically evaluating the effectiveness of security policies and controls, acting to address any identified weaknesses is a fundamental activity that allows an organization to manage its information security risks cost-effectively, rather than reacting to individual problems only after a violation has been detected or an audit finding has been reported. FISMA directs agencies to establish a process for remediating identified weaknesses in their information security policies and procedures. When weaknesses are identified, agencies are required to follow OMB and NIST guidance for developing and maintaining a plan of action and milestones. NIST Special Publication 800-37 states that remediation plans need to be updated to address weaknesses identified as a result of periodic testing. Key to an effective remediation plan is the accurate and complete inclusion of weaknesses identified during periodic testing. Remediation plans (also referred to as plans of action and milestones) should list all identified weaknesses and show estimated resource needs or other challenges to resolving them, key milestones and completion dates, and the status of corrective actions.

In their fiscal year 2006 FISMA reports, the IGs at all four departments reported that the departments did not consistently use the remediation plan process to manage the correction of their information security actions. Specifically, the four departments had not fully ensured (1) that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources or (2) that when an IT security weakness is identified, program officials develop, implement, and manage plans of action and milestones for their systems. Table 7 lists the challenges identified by the four departments and IGs regarding why they struggle to effectively handle deficiencies in information security policies, procedures, and practices.

Table 7: Challenges Departments Face in Developing Remediation Policies

Department	Challenges
Defense	• Ensuring its guidance aligns with NIST guidance • Aggregating data across components • Ensuring plans of action and milestones are developed and followed up • Developing an effective tool for its remediation process
Homeland Security	• Ensuring consistent implementation of its remediation process tool across components • Locating and tracking the information that is contained within its remediation tracking tool • Fixing or decommissioning the antiquated systems or systems not in use
Justice	• Ensuring data are accurate and complete for sensitive but unclassified systems • Validating data in its remediation system • Removing redundant plans of action and milestones from its database
State	• Monitoring and validating entries included in its remediation tracking tool

Source: GAO analysis of agency-reported data.

Although the four departments have control monitoring and weakness remediation processes in place, each department faces barriers to effectively incorporating these processes into their departmentwide information security programs:

- Defense officials reported that the size of the department has made it difficult to overcome its challenges in developing remediation plans. However, Defense is in the process of developing a departmentwide remediation process, but the process has not been completed and promulgated in final form. Interim guidance has been issued, and the Defense CIO stated that more time is needed to coordinate staffing to complete the final remediation guidance. Without complete guidance and an established departmentwide process, Defense cannot be assured that identified security weaknesses have been tracked and corrected.

- At Homeland Security, component agencies view the departmentwide FISMA reporting tool as more of a hindrance than a help for tracking their weaknesses, so use of the tool is inconsistent across component agencies. However, the department headquarters disagrees with the components on the usefulness of the tool. Unless the department can achieve user acceptance of this tool, it will be challenged to establish a consistent departmentwide remediation process.

- At Justice, the transition from an earlier NIST control framework to that in the most recent guidance[7] resulted in duplicate versions of plans of action and milestones (one for each framework). According to Justice officials, the department's tool for tracking these plans does not permit easy reconciliation of these redundancies because there is no automated process in place to do so. As a result, the department is challenged in accurately tracking information security weaknesses. Without such accurate tracking, the department has little assurance that security weaknesses are being addressed appropriately.

- In September 2006, State's IG stated that the department has not yet verified that IT security findings and recommendations from external and internal reviews are being addressed and resolved as part of the remediation process. The department is aware of the need to have all data in its tracking tool—including weaknesses reportable via the remediation process—monitored and validated on a regular basis. To address this issue in fiscal year 2007, the senior agency information security officer plans to use a "system vulnerability checklist" to ensure that system owners are aware of the weaknesses and plan to remediate them in a timely manner according to the set milestones. If properly implemented, such a process could help to ensure that identified security weaknesses have been tracked and corrected.

Certification and Accreditation Processes Show Weaknesses at Three Departments

OMB has established a certification and accreditation process for federal agencies that supports the establishment of the information security programs required by FISMA. This process requires various activities, including assessing system risk, documenting security controls in place and planned, testing controls in place, and analyzing test results.[8] Such a process provides a basis on which a senior agency official decides whether or not to approve system operation. Requiring such approvals from senior officials helps to ensure that risk is considered in the context of departmentwide mission operations.

[7] Initially, NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems* (Washington, D.C.: November 2001), provided the information security control framework for federal agencies. It was replaced in 2006 by the information security control framework described in NIST Special Publication 800-53.

[8] This process also requires, among other things, that security planning be documented. Such documentation includes risk assessments, contingency plans, incident response plans, security awareness and training plans, information systems rules of behavior, configuration management plans, security configuration checklists, privacy impact assessments, and system interconnection agreements.

However, as seen in table 8, three of the four departments reported that not all systems in their inventory are fully certified and accredited, and two of the four departments' IGs rated their respective department's certification and accreditation process as "poor." Only Justice overcame its challenges of prior years and achieved success in this activity.

Table 8: Status of System Certification and Accreditation at the Four Departments

Department	Agency-reported percentage of systems certified and accredited in fiscal year 2006	IG fiscal year 2006 assessment of agency certification and accreditation process
Defense	81%	Poor
Homeland Security	85	Satisfactory
Justice	100	Good
State	91	Poor

Sources: Agency- and IG-reported data.

According to Defense officials, the reason for the low percentage reported is that many of these systems received interim authority to operate, which is not reflected in the reported numbers.[9] Defense considers such interim authorities appropriate for certain systems, such as legacy systems and battlefield systems. However, systems without a full authorization to operate are an increased risk to agencywide operations, contributing to the overall risk to the agency.

In fiscal years 2005 and 2006, the Homeland Security IG reported that the data contained in the department's tracking tool used for monitoring the certification and accreditation process were often either incomplete or insufficient. In addition, in Homeland Security's effort to produce complete certification and accreditation documentation to satisfy federal requirements, the department's IG judged that the quality of work performed and documented did not meet applicable criteria. The IG has made recommendations to improve the quality of all certification and accreditation documents.

[9] If systems are shown to have an acceptable level or risk, they may receive authorization to operate; if not, authorization may be denied. The approving official may also give systems an interim authorization to operate. If systems are shown to have an acceptable level of residual risk after controls are implemented to mitigate unacceptable vulnerabilities, they may then receive a full authorization to operate.

In September 2006, the State IG reported that the department's bureaus performed certification and accreditation of their respective systems, and that two components (Information Resource Management and Diplomatic Security) also performed certification and accreditation on both applications and systems. The IG believed that the certification and accreditation process was fragmented and did not enable the department to adequately verify that all potential vulnerabilities are being addressed. The IG recommended that the CIO assign one entity the responsibility to manage the certification and accreditation process. Accordingly, the department now has an effort under way to address the inconsistencies in its certification and accreditation process, which has received positive feedback from internal stakeholders. Although we have not evaluated the new process, if it is implemented consistently across the department, it could reduce potential risks to the department's information systems.

Conclusions

Defense, Homeland Security, Justice, and State face challenges in implementing key information security control activities required by FISMA and OMB, which include maintaining complete and accurate system inventories, implementing common security configurations for all system platforms, training personnel, establishing and consistently implementing complete policies and processes for testing security controls, and fully certifying and accrediting information systems. The challenges in implementing these requirements arose from various weaknesses, including inadequate tools and gaps or inconsistencies in guidance.

These departments recognize the need to improve their implementation processes and have begun various steps to do so. For example, State is addressing the inconsistencies with its certification and accreditation process, and Defense is in the process of developing a departmentwide remediation process. Until each department improves its performance of key FISMA activities, the likelihood of fully implementing an effective information security program is diminished.

Recommendations for Executive Action

To assist the Departments of Defense, Homeland Security, Justice, and State in addressing challenges to implementing FISMA requirements, we are making the following 15 recommendations.

We recommend that the Secretary of Defense direct the Department of Defense's CIO to take the following six actions:

- Develop and implement a plan with milestones to finalize and implement a departmentwide definition of a major information system that is accepted by the Defense IG.
- Develop and implement a plan with milestones to achieve full implementation of common security configurations across all system platforms.
- Develop and implement a plan with milestones to implement a mechanism to track information security training of personnel (i.e., security awareness and specialized training).
- Address the weaknesses in security control testing policies as described in this report, and ensure that components complete required annual security control and contingency plan testing on all systems.
- Complete development of the departmentwide remediation process and finalize the remediation guidance.
- Develop and implement a plan with milestones to ensure that all information systems receive a full authorization to operate, and to improve the department's certification and accreditation process.

We recommend that the Secretary of Homeland Security direct the Department of Homeland Security's CIO to take the following four actions:

- Develop and implement a plan with milestones to achieve full implementation of common security configurations across all system platforms.
- Coordinate with Homeland Security's Office of Human Capital to finalize implementation of the centralized Web-based learning management system for tracking the information security training of personnel.
- Address the weaknesses in security control testing policies as described in this report, and ensure that components complete required annual security control and contingency plan testing on all systems.
- Determine whether the department's FISMA reporting tool meets the requirements of different users, such as those at components, and take any necessary corrective action.

We recommend that the Attorney General direct the Department of Justice's CIO to take the following three actions:

- Develop and implement a plan with milestones to achieve full implementation of common security configurations across all system platforms.
- Address the weaknesses in security control testing policies as described in this report.
- Reconcile redundancies in the department's remediation plan tracking tool.

Finally, we recommend that the Secretary of State direct State's CIO to take the following two actions:

- Improve mechanisms for tracking information security awareness training of personnel.
- Address the weaknesses in security control testing policies as described in this report, and ensure that components complete required annual security control and contingency plan testing on all systems.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from Defense's Deputy Assistant Secretary of Defense Information and Identity Assurance (reproduced in app. II), from the Director of Homeland Security's Departmental GAO/OIG Liaison Office (reproduced in app. III), from Justice's Assistant Attorney General for Administration (reproduced in app. IV), and from State's Assistant Secretary for Resource Management and Chief Financial Officer (reproduced in app. V). In these comments, officials from Homeland Security, Justice, and State generally agreed with our recommendations to their respective departments, and stated that they had implemented or were in the process of implementing them. Defense generally agreed with two recommendations, partially agreed with a third, and did not agree with the other three. All four departments provided technical comments, which we have incorporated as appropriate.

In its comments, Defense did not concur with our recommendation to develop and implement a departmentwide definition of a major information system that is accepted by the Defense IG. Defense stated that it has a standard definition for FISMA reporting and has informed the Defense IG that it will continue to use the definition in the annual data call. While Defense does have a definition of a major information system specified in its annual IT repository guidance, as we discuss in our report, Defense's own guidance provides at least two definitions of a system. This forces the components, and the Defense IG, to make independent interpretations of what should be included in the inventory for FISMA reporting purposes, leading to inconsistent results. Thus, we continue to believe our recommendation has merit.

Defense partially concurred with our recommendation to achieve full implementation of common security configurations across all system platforms, noting that it was spearheading a federal initiative and that the policy is planned for implementation by February 2008. Defense concurred in principle with our recommendation to implement a mechanism to track information security training of personnel and stated that the department has already initiated actions to complete the recommendation. Defense also concurred in principle with our recommendation to address the weaknesses in security control testing policies and ensure that components complete required security control and contingency plan testing for all systems.

Defense did not concur with our recommendation to complete the development of the departmentwide remediation process and finalize the remediation guidance. However, officials commented that the interim guidance, discussed in our report, will be finalized in September 2007. Defense also did not concur with our recommendation to ensure that all information systems receive a full authorization to operate and to improve the department's certification and accreditation process. Defense stated that it believes an interim authorization to operate represents a sound risk management practice and balances operational requirements with acceptable risk, while further noting that its combined interim and full authorizations to operate total 91.9 percent of Defense systems. Although interim authorizations to operate represent some level of accepting risk, we believe that without a full authorization to operate, there is an increased risk to the department's operations and continue to believe our recommendation has merit.

In addition, Defense stated that the report does not accurately reflect the current security posture of the department and the progress it has made in implementing the provisions of FISMA. Throughout our report, where appropriate, we acknowledge the progress made by the department in implementing the provisions of FISMA and have deleted certain outdated information contained in the draft report. Nonetheless, Defense still faces challenges in individual areas of FISMA as noted in our report.

In its comments, Homeland Security noted that the report does not provide common solutions that could be applied to large agencies across the federal government. Our review was not governmentwide in scope; rather, it was limited to challenges faced by Defense, Homeland Security, Justice, and State. Accordingly, our recommendations are addressed individually to these four departments.

State also provided several comments related to the contents of our report. First, the department did not agree with the report's implication that the issues associated with the recommendations serve as challenges or obstacles that inhibit the implementation of FISMA. Rather, State characterizes them as weaknesses that are receiving the proper attention. We believe that the issues identified in our report are appropriately characterized as the challenges State faces with regard to verifying whether all of its employees received the required FISMA security awareness training and with regard to certifying and accrediting its systems. Our report also discusses the progress State has made in these two areas.

Second, in response to the recommendation to improve mechanisms for tracking information security awareness training of all personnel, State asserted that the report declared that it is unable to identify all of its employees. However, our report does not make this claim; instead, we note that State has not been able to verify that all of its employees and contractors have received the required training.

Finally, State also noted in its comments that prior GAO reports and testimonies discussed the lack of a common IG reporting framework and that current FISMA reporting does not take full account of an agency's ability to detect, respond to, and react to cyber security threats and manage vulnerabilities. While State officials told us that these issues inhibit the department from implementing the provisions of FISMA, we emphasize that despite external factors, which may influence measurement or perception of an agency's performance, the department still controlled the internal processes that effectively execute all of the information security program activities required by FISMA, which constituted the scope of this report. These issues were addressed, as noted by State in its comments, on a governmentwide basis in other GAO reports and testimonies that had a broader scope.

As we agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies of this report to interested congressional committees; the Secretaries of Defense, Homeland Security, and State; and the U.S. Attorney General. We will also make copies available to others on 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 VI.

Sincerely yours,

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objective, Scope, and Methodology

Our objective was to determine the challenges or obstacles that inhibit the implementation of the information security provisions of the Federal Information Security Management Act of 2002 (FISMA) at the Departments of Defense, Homeland Security, Justice, and State.

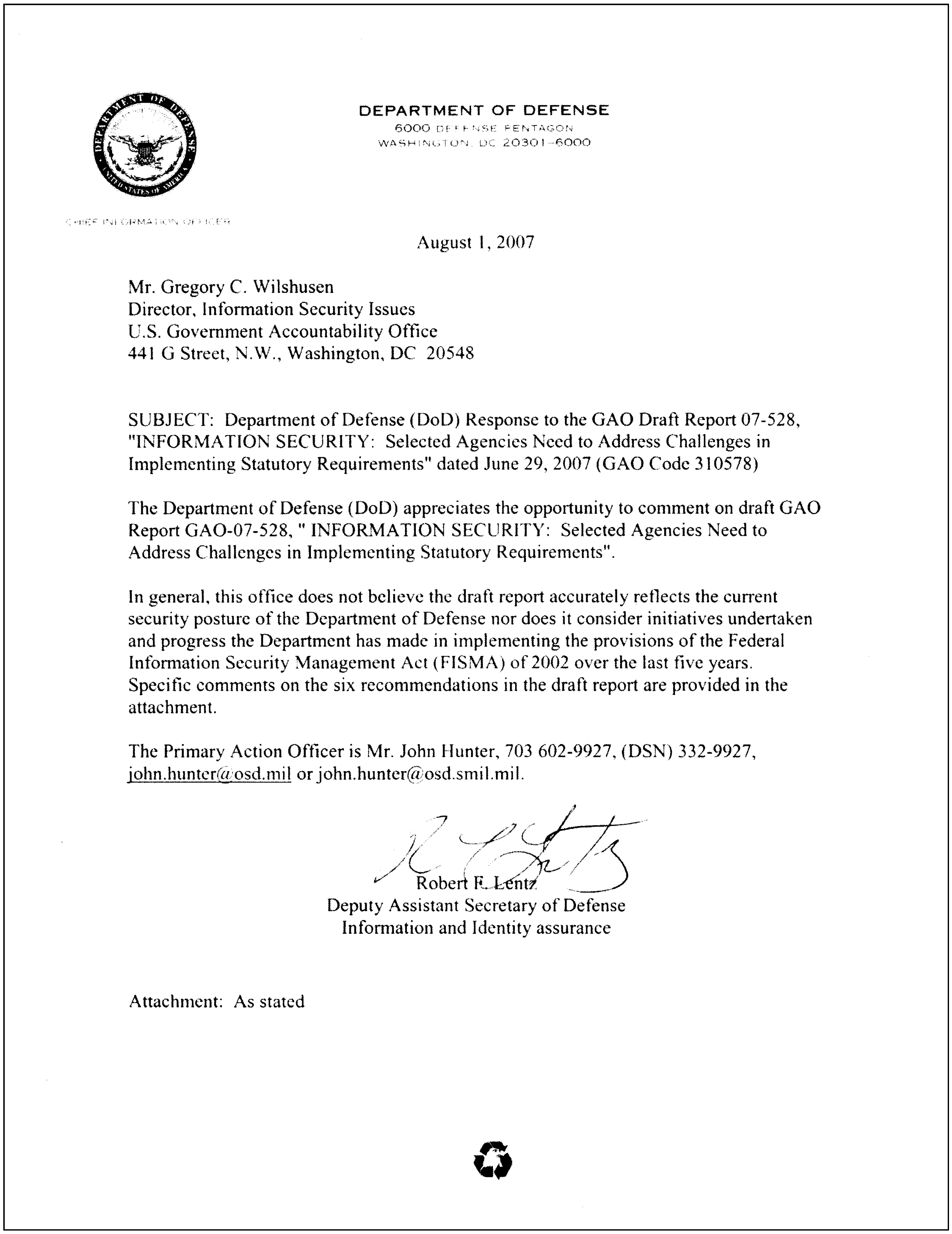
To do this, we reviewed and analyzed FISMA (Public Law 107-347) and mapped these requirements to (1) National Institute of Standards and Technology (NIST) guidelines and (2) Office of Management and Budget (OMB) reporting requirements. We also reviewed and analyzed relevant NIST special publications and federal information processing standards that were created and modified due to FISMA, as well as guidance and reports issued by OMB. For example, we reviewed and analyzed its *Fiscal Year 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002* and OMB Circular A-130, *Management of Federal Information Resources*. In addition, we reviewed our previous information security work. We also interviewed individuals from OMB's Office of Information and Regulatory Affairs and Office of General Counsel and interviewed officials from the NIST Computer Security Division to discuss their FISMA implementation project work as mandated by FISMA.

We also reviewed and analyzed chief information officer (CIO) and inspectors general FISMA reports for fiscal years 2003 through 2006 at Defense, Homeland Security, Justice, and State. In addition, we reviewed and analyzed various plans, policies, and procedures at the four departments. These included strategic plans, risk management policies, and budget documentation. We also held structured interviews with individuals who had FISMA implementation as their primary responsibility at each department and at selected department components. Specifically, at Defense we interviewed individuals from the Office of the Secretary of Defense as well as three Defense service components—the Departments of the Army and Navy, and the U.S. Air Force—and individuals from the Defense Information Systems Agency. At Homeland Security, we interviewed officials within the Office of the CIO as well as from the U.S. Coast Guard, Federal Emergency Management Agency, U.S. Citizenship and Immigration Services, Transportation Security Administration, and U.S. Immigration and Customs Enforcement. At Justice, we interviewed officials within the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Justice Management Division; the Federal Bureau of Investigation; the Executive Office of United States Attorneys; and the Drug Enforcement Administration. At State, we interviewed officials of the Office of the Chief Information Officer, the Office of Foreign Missions, the Bureau of Diplomatic Security, and the Bureau of Information Resources

Management. Finally, we met with the Office of the Inspector General at each of the four departments to discuss what challenges its department has encountered in implementing FISMA.

Our work was conducted in Washington, D.C., from July 2006 through May 2007. All work was performed in accordance with generally accepted government auditing standards.

Appendix II: Comments from the Department of Defense



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

August 1, 2007

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

SUBJECT: Department of Defense (DoD) Response to the GAO Draft Report 07-528, "INFORMATION SECURITY: Selected Agencies Need to Address Challenges in Implementing Statutory Requirements" dated June 29, 2007 (GAO Code 310578)

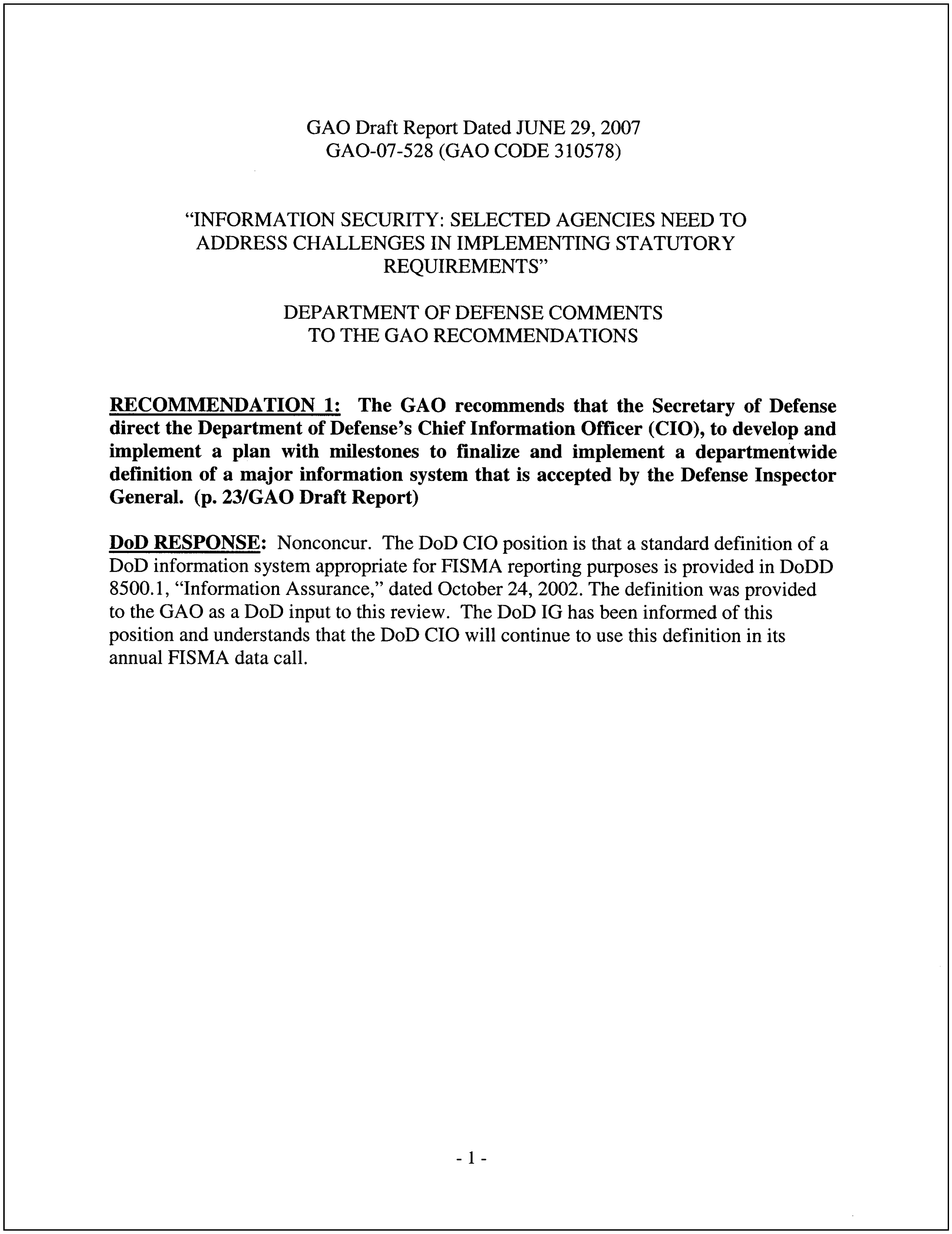
The Department of Defense (DoD) appreciates the opportunity to comment on draft GAO Report GAO-07-528, " INFORMATION SECURITY: Selected Agencies Need to Address Challenges in Implementing Statutory Requirements".

In general, this office does not believe the draft report accurately reflects the current security posture of the Department of Defense nor does it consider initiatives undertaken and progress the Department has made in implementing the provisions of the Federal Information Security Management Act (FISMA) of 2002 over the last five years. Specific comments on the six recommendations in the draft report are provided in the attachment.

The Primary Action Officer is Mr. John Hunter, 703 602-9927, (DSN) 332-9927, john.hunter@osd.mil or john.hunter@osd.smil.mil.

Robert F. Lentz
Deputy Assistant Secretary of Defense
Information and Identity assurance

Attachment: As stated



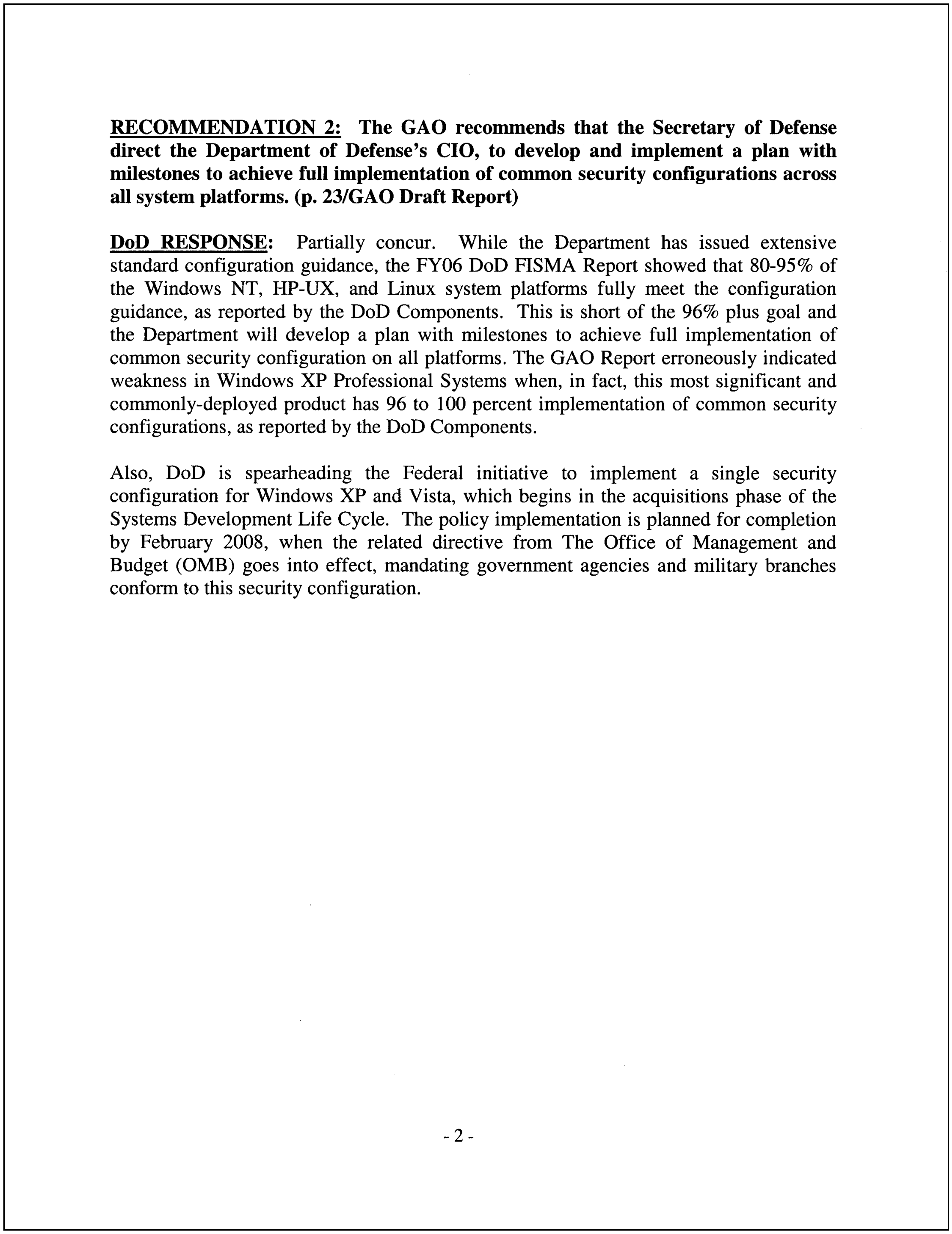
GAO Draft Report Dated JUNE 29, 2007
GAO-07-528 (GAO CODE 310578)

"INFORMATION SECURITY: SELECTED AGENCIES NEED TO ADDRESS CHALLENGES IN IMPLEMENTING STATUTORY REQUIREMENTS"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

<u>RECOMMENDATION 1:</u> The GAO recommends that the Secretary of Defense direct the Department of Defense's Chief Information Officer (CIO), to develop and implement a plan with milestones to finalize and implement a departmentwide definition of a major information system that is accepted by the Defense Inspector General. (p. 23/GAO Draft Report)

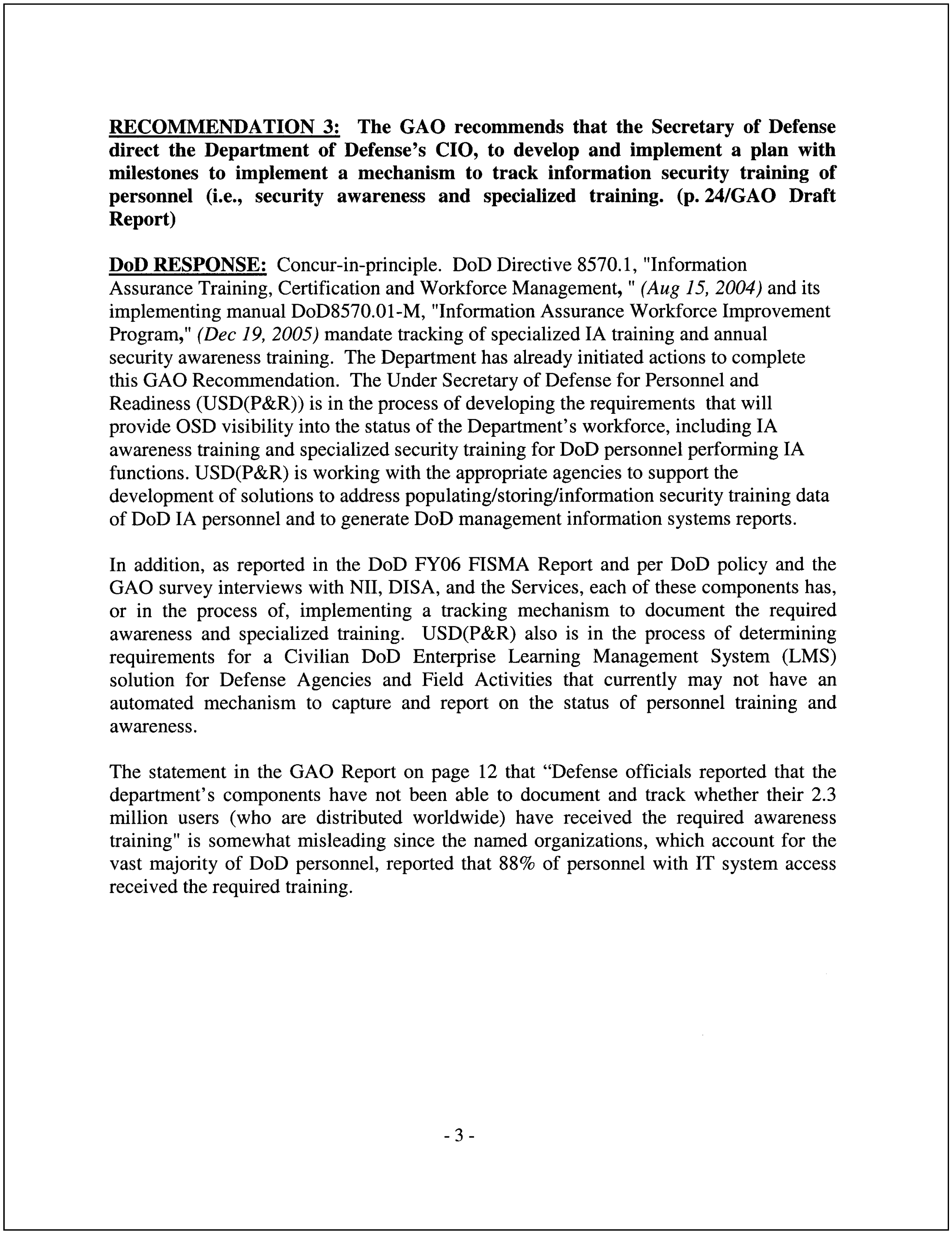
<u>DoD RESPONSE</u>: Nonconcur. The DoD CIO position is that a standard definition of a DoD information system appropriate for FISMA reporting purposes is provided in DoDD 8500.1, "Information Assurance," dated October 24, 2002. The definition was provided to the GAO as a DoD input to this review. The DoD IG has been informed of this position and understands that the DoD CIO will continue to use this definition in its annual FISMA data call.



<u>RECOMMENDATION 2:</u> The GAO recommends that the Secretary of Defense direct the Department of Defense's CIO, to develop and implement a plan with milestones to achieve full implementation of common security configurations across all system platforms. (p. 23/GAO Draft Report)

<u>DoD RESPONSE</u>: Partially concur. While the Department has issued extensive standard configuration guidance, the FY06 DoD FISMA Report showed that 80-95% of the Windows NT, HP-UX, and Linux system platforms fully meet the configuration guidance, as reported by the DoD Components. This is short of the 96% plus goal and the Department will develop a plan with milestones to achieve full implementation of common security configuration on all platforms. The GAO Report erroneously indicated weakness in Windows XP Professional Systems when, in fact, this most significant and commonly-deployed product has 96 to 100 percent implementation of common security configurations, as reported by the DoD Components.

Also, DoD is spearheading the Federal initiative to implement a single security configuration for Windows XP and Vista, which begins in the acquisitions phase of the Systems Development Life Cycle. The policy implementation is planned for completion by February 2008, when the related directive from The Office of Management and Budget (OMB) goes into effect, mandating government agencies and military branches conform to this security configuration.

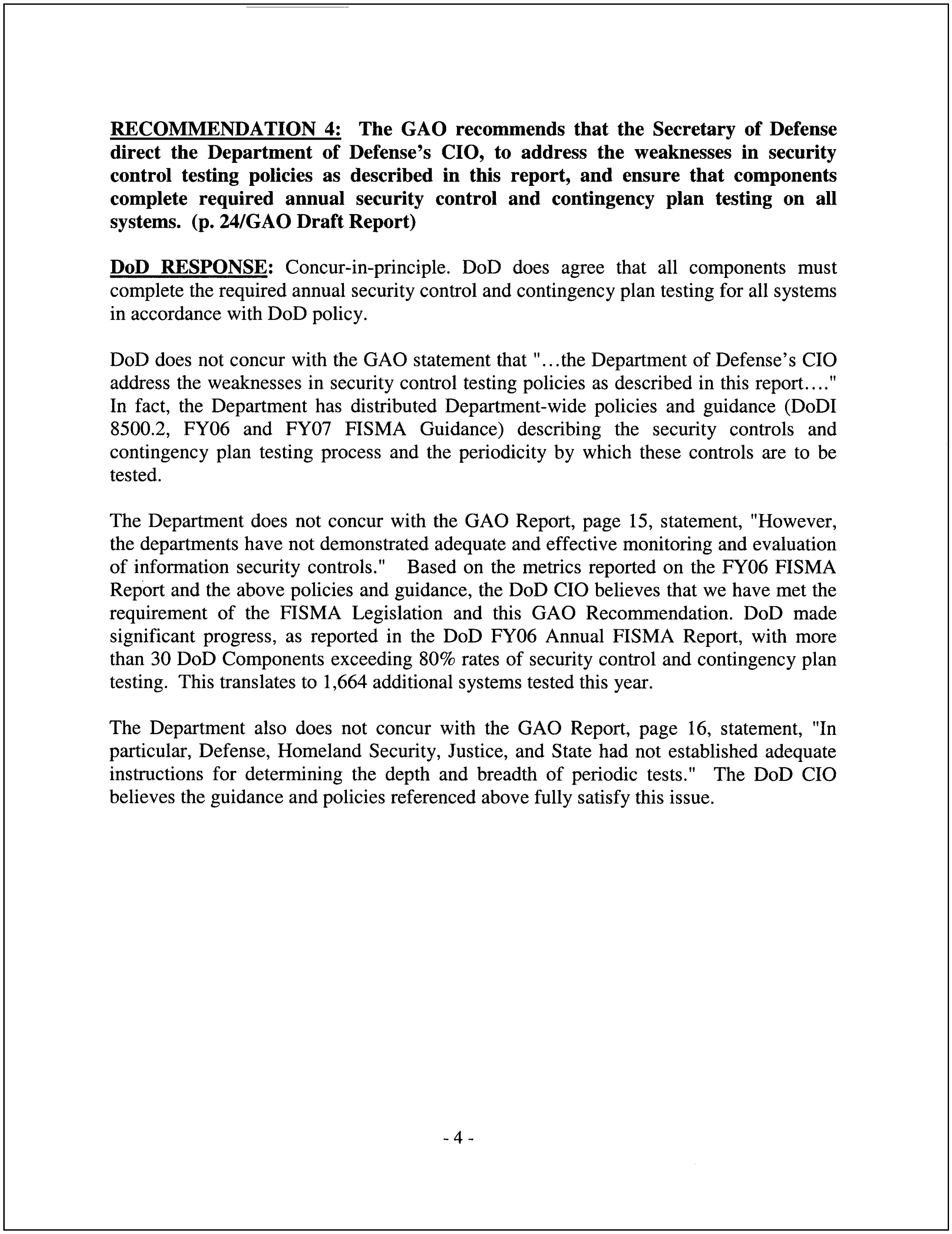


RECOMMENDATION 3: **The GAO recommends that the Secretary of Defense direct the Department of Defense's CIO, to develop and implement a plan with milestones to implement a mechanism to track information security training of personnel (i.e., security awareness and specialized training. (p. 24/GAO Draft Report)**

DoD RESPONSE: Concur-in-principle. DoD Directive 8570.1, "Information Assurance Training, Certification and Workforce Management, " *(Aug 15, 2004)* and its implementing manual DoD8570.01-M, "Information Assurance Workforce Improvement Program," *(Dec 19, 2005)* mandate tracking of specialized IA training and annual security awareness training. The Department has already initiated actions to complete this GAO Recommendation. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) is in the process of developing the requirements that will provide OSD visibility into the status of the Department's workforce, including IA awareness training and specialized security training for DoD personnel performing IA functions. USD(P&R) is working with the appropriate agencies to support the development of solutions to address populating/storing/information security training data of DoD IA personnel and to generate DoD management information systems reports.

In addition, as reported in the DoD FY06 FISMA Report and per DoD policy and the GAO survey interviews with NII, DISA, and the Services, each of these components has, or in the process of, implementing a tracking mechanism to document the required awareness and specialized training. USD(P&R) also is in the process of determining requirements for a Civilian DoD Enterprise Learning Management System (LMS) solution for Defense Agencies and Field Activities that currently may not have an automated mechanism to capture and report on the status of personnel training and awareness.

The statement in the GAO Report on page 12 that "Defense officials reported that the department's components have not been able to document and track whether their 2.3 million users (who are distributed worldwide) have received the required awareness training" is somewhat misleading since the named organizations, which account for the vast majority of DoD personnel, reported that 88% of personnel with IT system access received the required training.



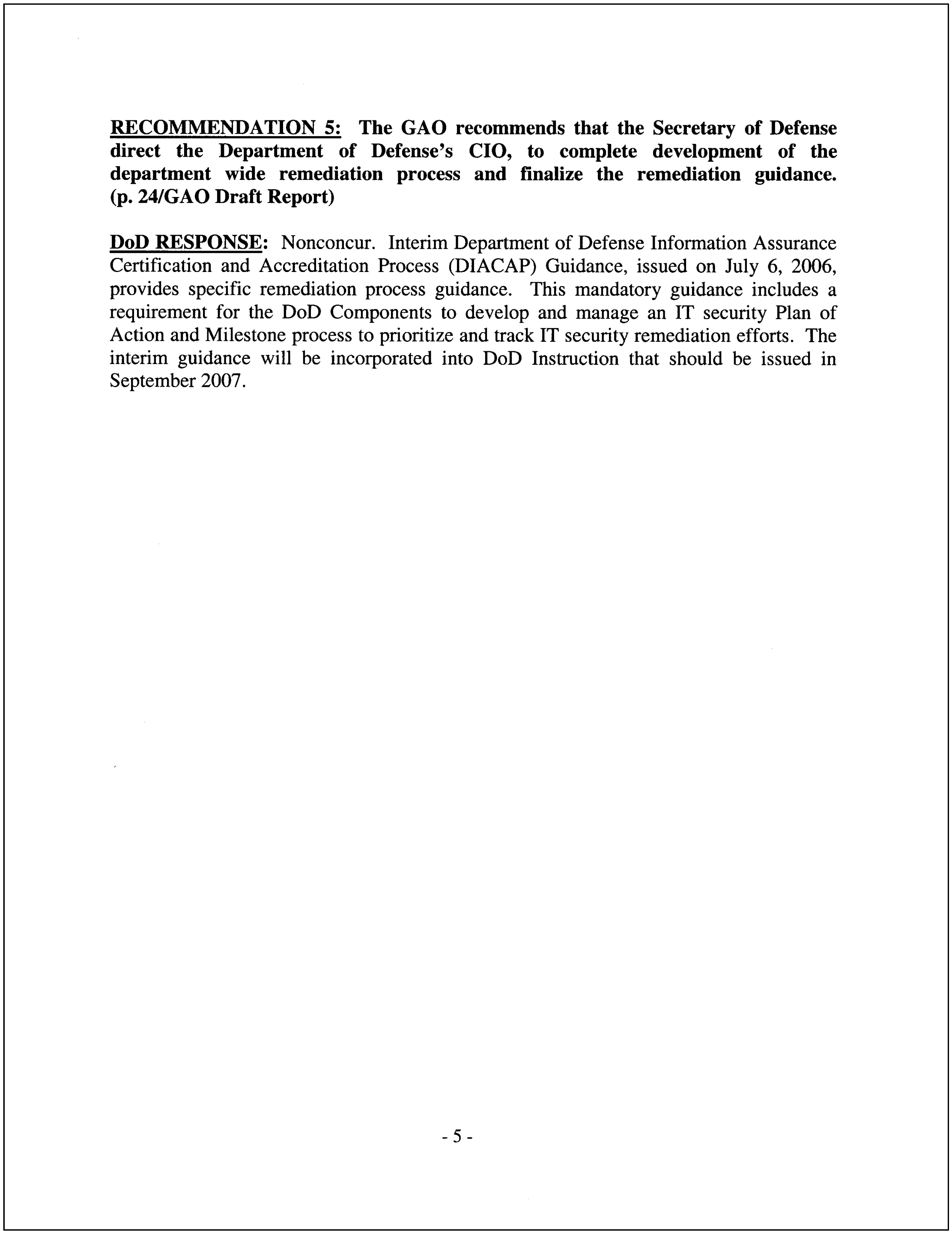
RECOMMENDATION 4: The GAO recommends that the Secretary of Defense direct the Department of Defense's CIO, to address the weaknesses in security control testing policies as described in this report, and ensure that components complete required annual security control and contingency plan testing on all systems. (p. 24/GAO Draft Report)

DoD RESPONSE: Concur-in-principle. DoD does agree that all components must complete the required annual security control and contingency plan testing for all systems in accordance with DoD policy.

DoD does not concur with the GAO statement that "...the Department of Defense's CIO address the weaknesses in security control testing policies as described in this report...." In fact, the Department has distributed Department-wide policies and guidance (DoDI 8500.2, FY06 and FY07 FISMA Guidance) describing the security controls and contingency plan testing process and the periodicity by which these controls are to be tested.

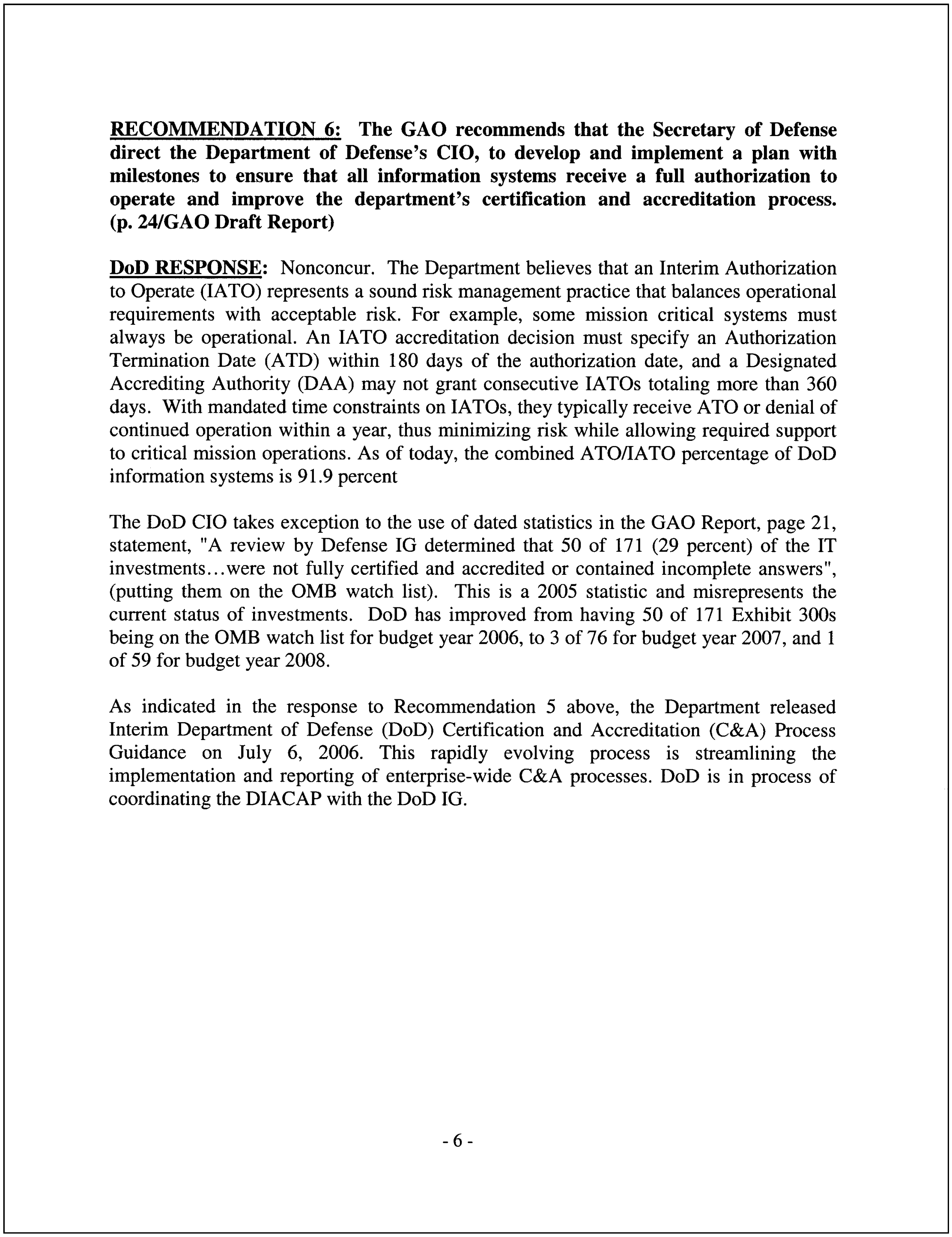
The Department does not concur with the GAO Report, page 15, statement, "However, the departments have not demonstrated adequate and effective monitoring and evaluation of information security controls." Based on the metrics reported on the FY06 FISMA Report and the above policies and guidance, the DoD CIO believes that we have met the requirement of the FISMA Legislation and this GAO Recommendation. DoD made significant progress, as reported in the DoD FY06 Annual FISMA Report, with more than 30 DoD Components exceeding 80% rates of security control and contingency plan testing. This translates to 1,664 additional systems tested this year.

The Department also does not concur with the GAO Report, page 16, statement, "In particular, Defense, Homeland Security, Justice, and State had not established adequate instructions for determining the depth and breadth of periodic tests." The DoD CIO believes the guidance and policies referenced above fully satisfy this issue.



<u>RECOMMENDATION 5:</u> The GAO recommends that the Secretary of Defense direct the Department of Defense's CIO, to complete development of the department wide remediation process and finalize the remediation guidance. (p. 24/GAO Draft Report)

<u>DoD RESPONSE</u>: Nonconcur. Interim Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Guidance, issued on July 6, 2006, provides specific remediation process guidance. This mandatory guidance includes a requirement for the DoD Components to develop and manage an IT security Plan of Action and Milestone process to prioritize and track IT security remediation efforts. The interim guidance will be incorporated into DoD Instruction that should be issued in September 2007.



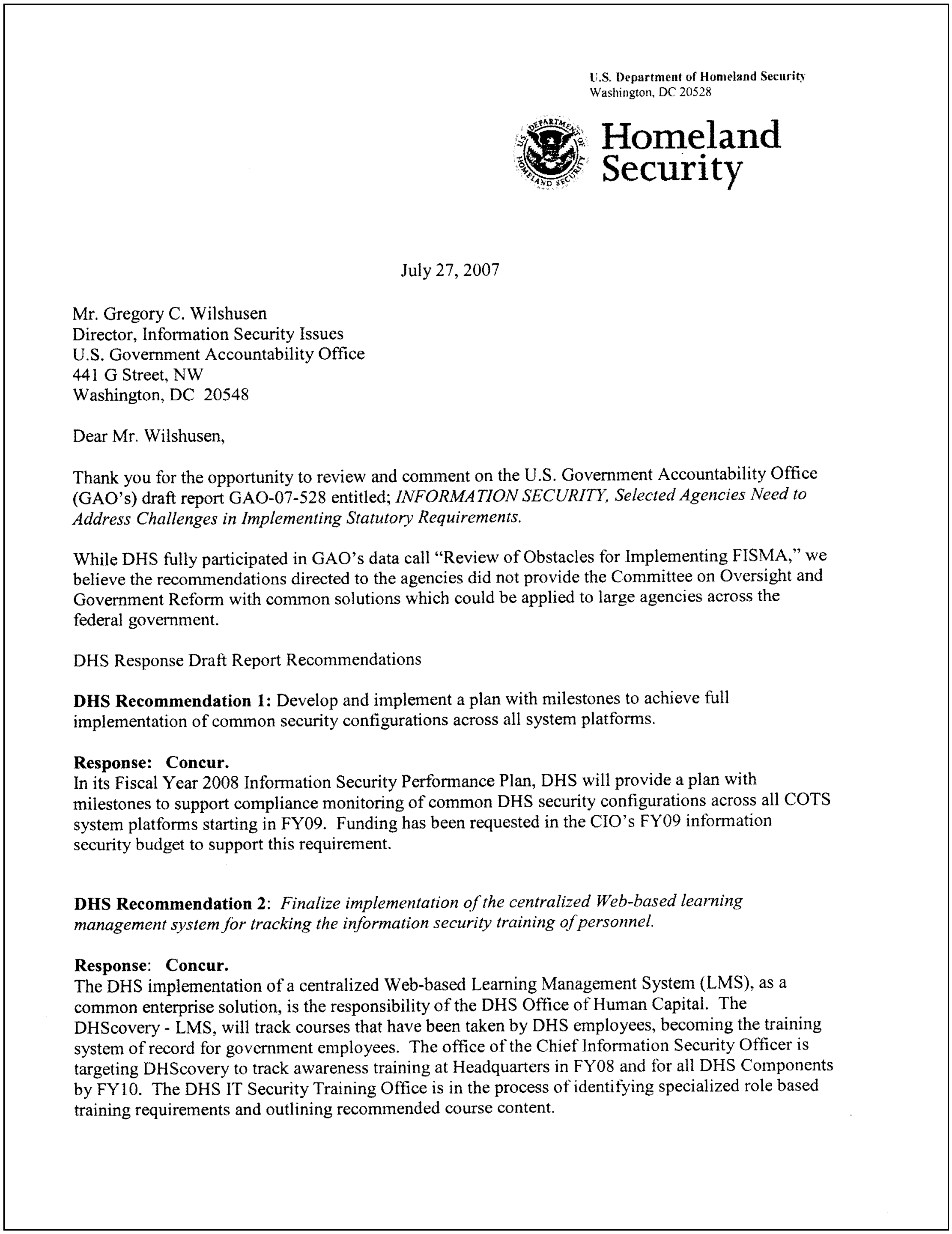
RECOMMENDATION 6: The GAO recommends that the Secretary of Defense direct the Department of Defense's CIO, to develop and implement a plan with milestones to ensure that all information systems receive a full authorization to operate and improve the department's certification and accreditation process. (p. 24/GAO Draft Report)

DoD RESPONSE: Nonconcur. The Department believes that an Interim Authorization to Operate (IATO) represents a sound risk management practice that balances operational requirements with acceptable risk. For example, some mission critical systems must always be operational. An IATO accreditation decision must specify an Authorization Termination Date (ATD) within 180 days of the authorization date, and a Designated Accrediting Authority (DAA) may not grant consecutive IATOs totaling more than 360 days. With mandated time constraints on IATOs, they typically receive ATO or denial of continued operation within a year, thus minimizing risk while allowing required support to critical mission operations. As of today, the combined ATO/IATO percentage of DoD information systems is 91.9 percent

The DoD CIO takes exception to the use of dated statistics in the GAO Report, page 21, statement, "A review by Defense IG determined that 50 of 171 (29 percent) of the IT investments...were not fully certified and accredited or contained incomplete answers", (putting them on the OMB watch list). This is a 2005 statistic and misrepresents the current status of investments. DoD has improved from having 50 of 171 Exhibit 300s being on the OMB watch list for budget year 2006, to 3 of 76 for budget year 2007, and 1 of 59 for budget year 2008.

As indicated in the response to Recommendation 5 above, the Department released Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance on July 6, 2006. This rapidly evolving process is streamlining the implementation and reporting of enterprise-wide C&A processes. DoD is in process of coordinating the DIACAP with the DoD IG.

Appendix III: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

July 27, 2007

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

Dear Mr. Wilshusen,

Thank you for the opportunity to review and comment on the U.S. Government Accountability Office (GAO's) draft report GAO-07-528 entitled; *INFORMATION SECURITY, Selected Agencies Need to Address Challenges in Implementing Statutory Requirements.*

While DHS fully participated in GAO's data call "Review of Obstacles for Implementing FISMA," we believe the recommendations directed to the agencies did not provide the Committee on Oversight and Government Reform with common solutions which could be applied to large agencies across the federal government.

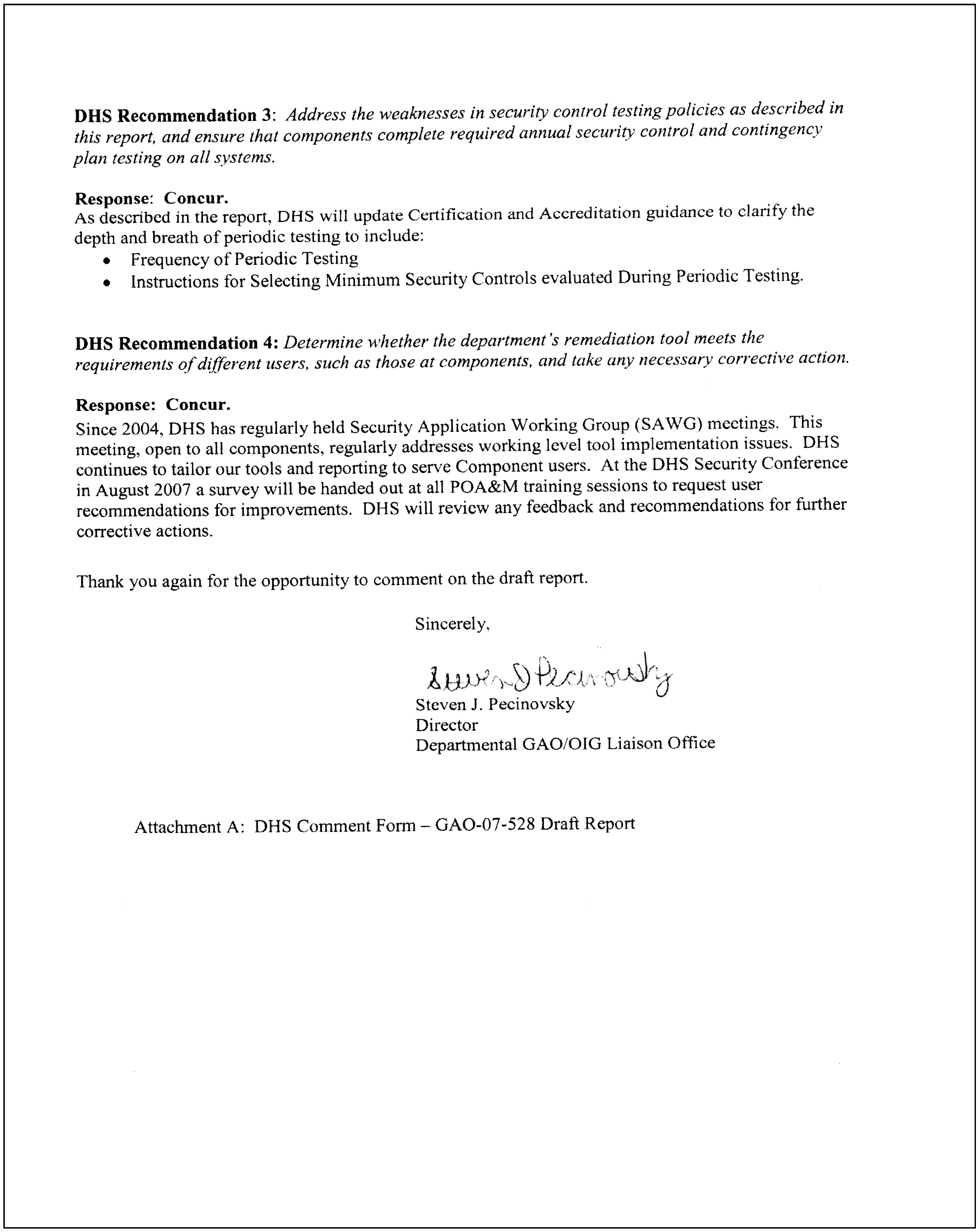
DHS Response Draft Report Recommendations

DHS Recommendation 1: Develop and implement a plan with milestones to achieve full implementation of common security configurations across all system platforms.

Response: Concur.
In its Fiscal Year 2008 Information Security Performance Plan, DHS will provide a plan with milestones to support compliance monitoring of common DHS security configurations across all COTS system platforms starting in FY09. Funding has been requested in the CIO's FY09 information security budget to support this requirement.

DHS Recommendation 2: *Finalize implementation of the centralized Web-based learning management system for tracking the information security training of personnel.*

Response: **Concur.**
The DHS implementation of a centralized Web-based Learning Management System (LMS), as a common enterprise solution, is the responsibility of the DHS Office of Human Capital. The DHScovery - LMS, will track courses that have been taken by DHS employees, becoming the training system of record for government employees. The office of the Chief Information Security Officer is targeting DHScovery to track awareness training at Headquarters in FY08 and for all DHS Components by FY10. The DHS IT Security Training Office is in the process of identifying specialized role based training requirements and outlining recommended course content.



DHS Recommendation 3: *Address the weaknesses in security control testing policies as described in this report, and ensure that components complete required annual security control and contingency plan testing on all systems.*

Response: Concur.
As described in the report, DHS will update Certification and Accreditation guidance to clarify the depth and breath of periodic testing to include:

- Frequency of Periodic Testing
- Instructions for Selecting Minimum Security Controls evaluated During Periodic Testing.

DHS Recommendation 4: *Determine whether the department's remediation tool meets the requirements of different users, such as those at components, and take any necessary corrective action.*

Response: Concur.
Since 2004, DHS has regularly held Security Application Working Group (SAWG) meetings. This meeting, open to all components, regularly addresses working level tool implementation issues. DHS continues to tailor our tools and reporting to serve Component users. At the DHS Security Conference in August 2007 a survey will be handed out at all POA&M training sessions to request user recommendations for improvements. DHS will review any feedback and recommendations for further corrective actions.

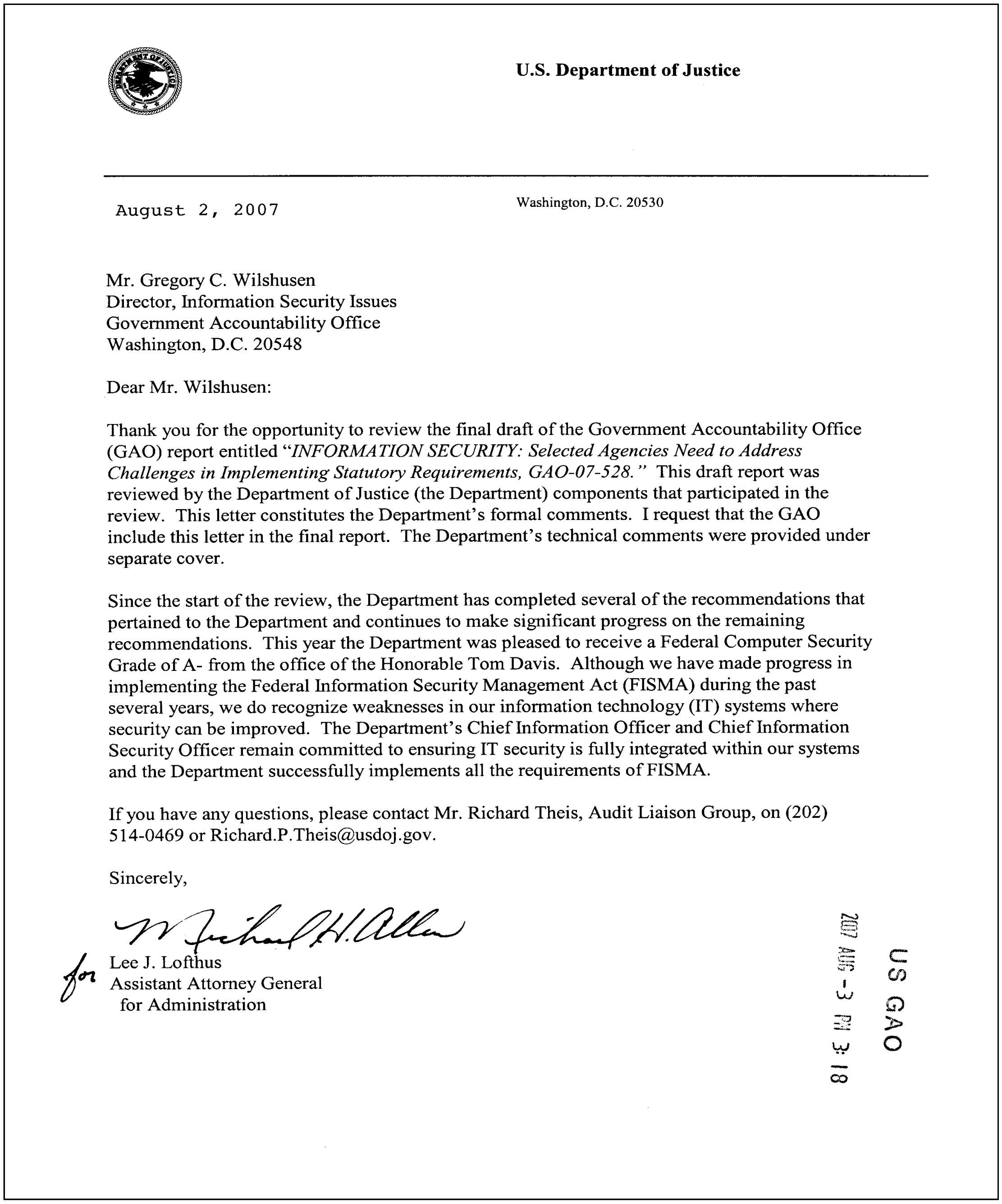
Thank you again for the opportunity to comment on the draft report.

Sincerely,

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

Attachment A: DHS Comment Form – GAO-07-528 Draft Report

Appendix IV: Comments from the Department of Justice



U.S. Department of Justice

August 2, 2007

Washington, D.C. 20530

Mr. Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office
Washington, D.C. 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review the final draft of the Government Accountability Office (GAO) report entitled "*INFORMATION SECURITY: Selected Agencies Need to Address Challenges in Implementing Statutory Requirements, GAO-07-528.*" This draft report was reviewed by the Department of Justice (the Department) components that participated in the review. This letter constitutes the Department's formal comments. I request that the GAO include this letter in the final report. The Department's technical comments were provided under separate cover.

Since the start of the review, the Department has completed several of the recommendations that pertained to the Department and continues to make significant progress on the remaining recommendations. This year the Department was pleased to receive a Federal Computer Security Grade of A- from the office of the Honorable Tom Davis. Although we have made progress in implementing the Federal Information Security Management Act (FISMA) during the past several years, we do recognize weaknesses in our information technology (IT) systems where security can be improved. The Department's Chief Information Officer and Chief Information Security Officer remain committed to ensuring IT security is fully integrated within our systems and the Department successfully implements all the requirements of FISMA.

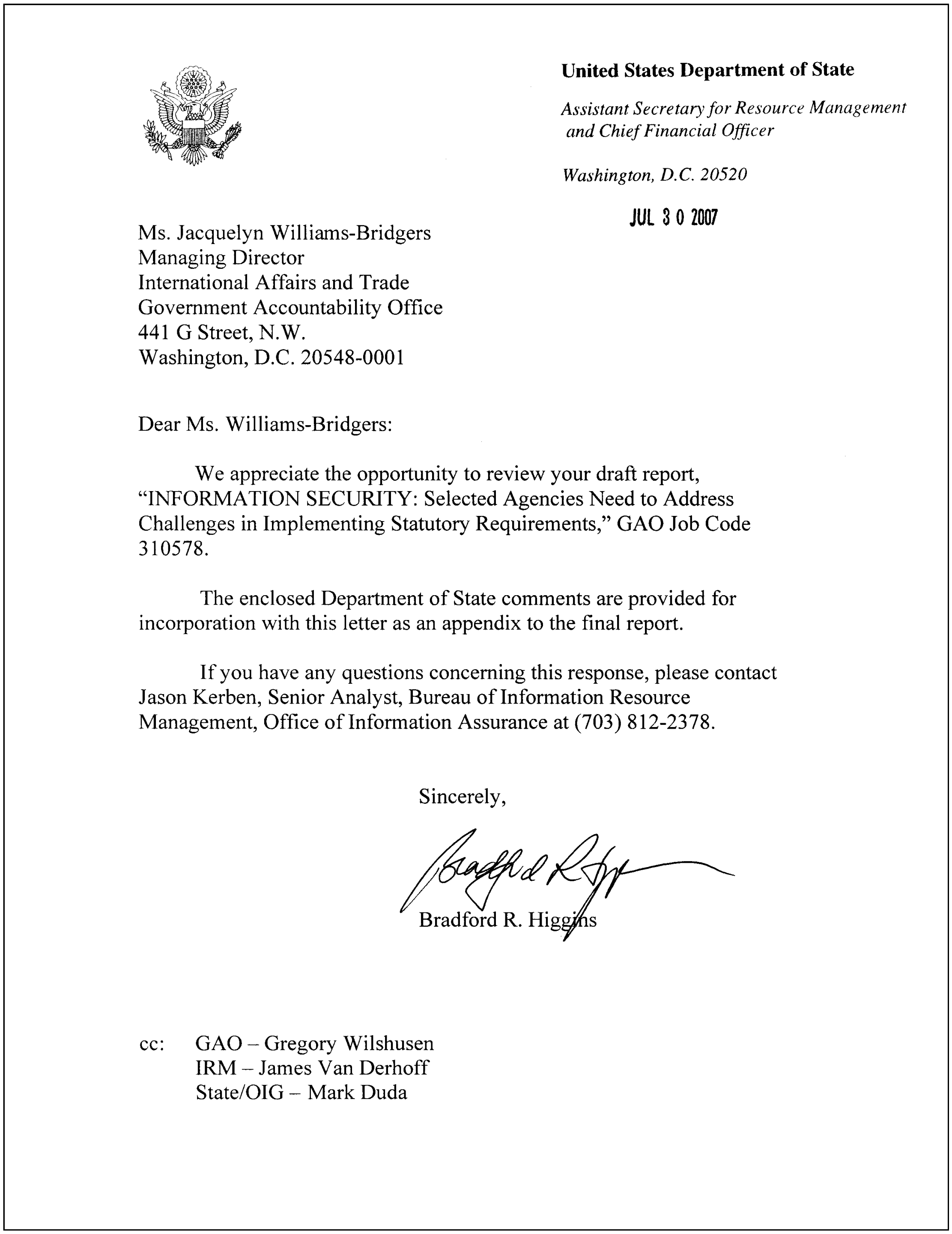
If you have any questions, please contact Mr. Richard Theis, Audit Liaison Group, on (202) 514-0469 or Richard.P.Theis@usdoj.gov.

Sincerely,

Michael H. Allen

for Lee J. Lofthus
Assistant Attorney General
for Administration

Appendix V: Comments from the Department of State



United States Department of State

Assistant Secretary for Resource Management
and Chief Financial Officer

Washington, D.C. 20520

JUL 3 0 2007

Ms. Jacquelyn Williams-Bridgers
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Ms. Williams-Bridgers:

We appreciate the opportunity to review your draft report, "INFORMATION SECURITY: Selected Agencies Need to Address Challenges in Implementing Statutory Requirements," GAO Job Code 310578.

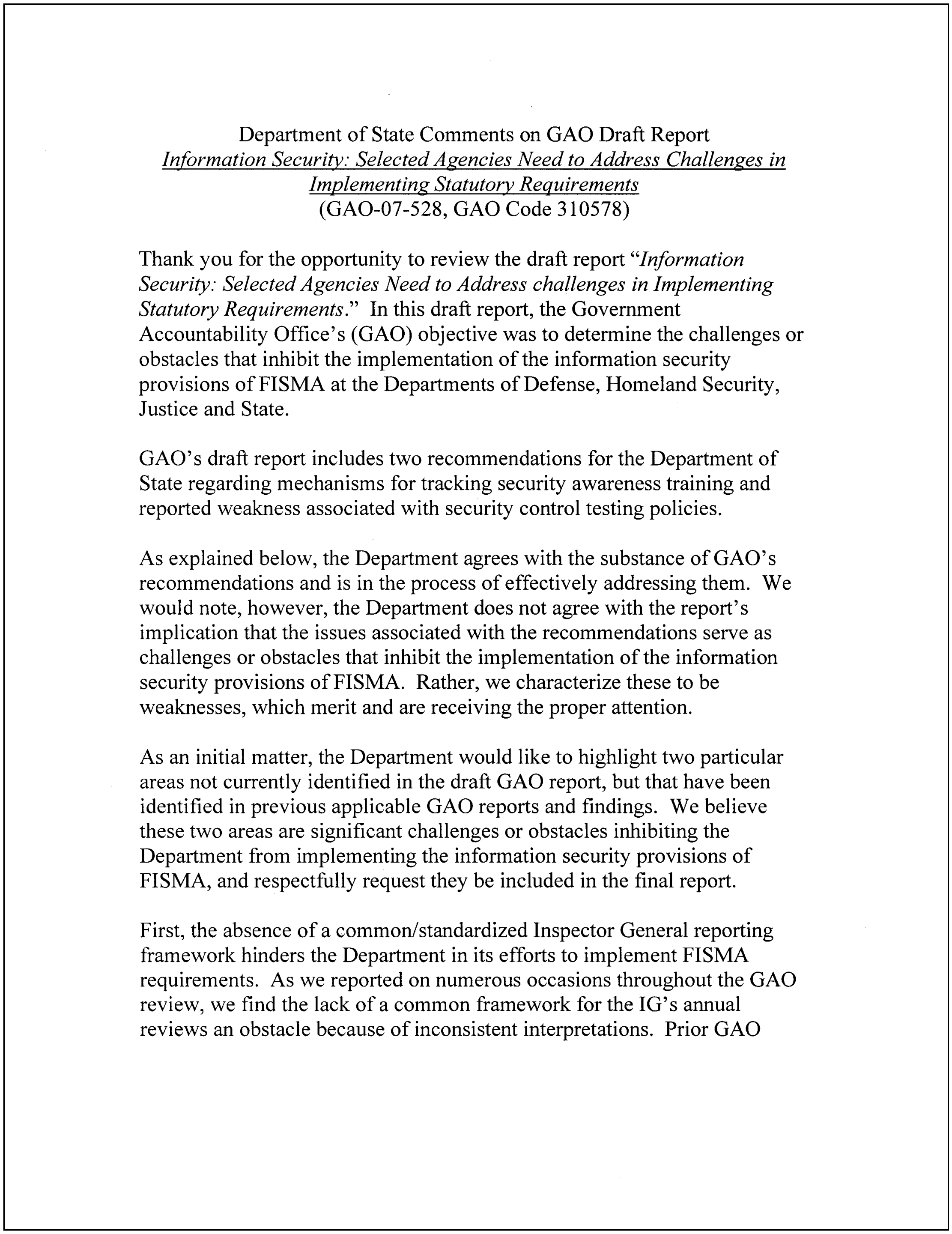
The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Jason Kerben, Senior Analyst, Bureau of Information Resource Management, Office of Information Assurance at (703) 812-2378.

Sincerely,

Bradford R. Higgins

cc: GAO – Gregory Wilshusen
IRM – James Van Derhoff
State/OIG – Mark Duda



Department of State Comments on GAO Draft Report
Information Security: Selected Agencies Need to Address Challenges in Implementing Statutory Requirements
(GAO-07-528, GAO Code 310578)

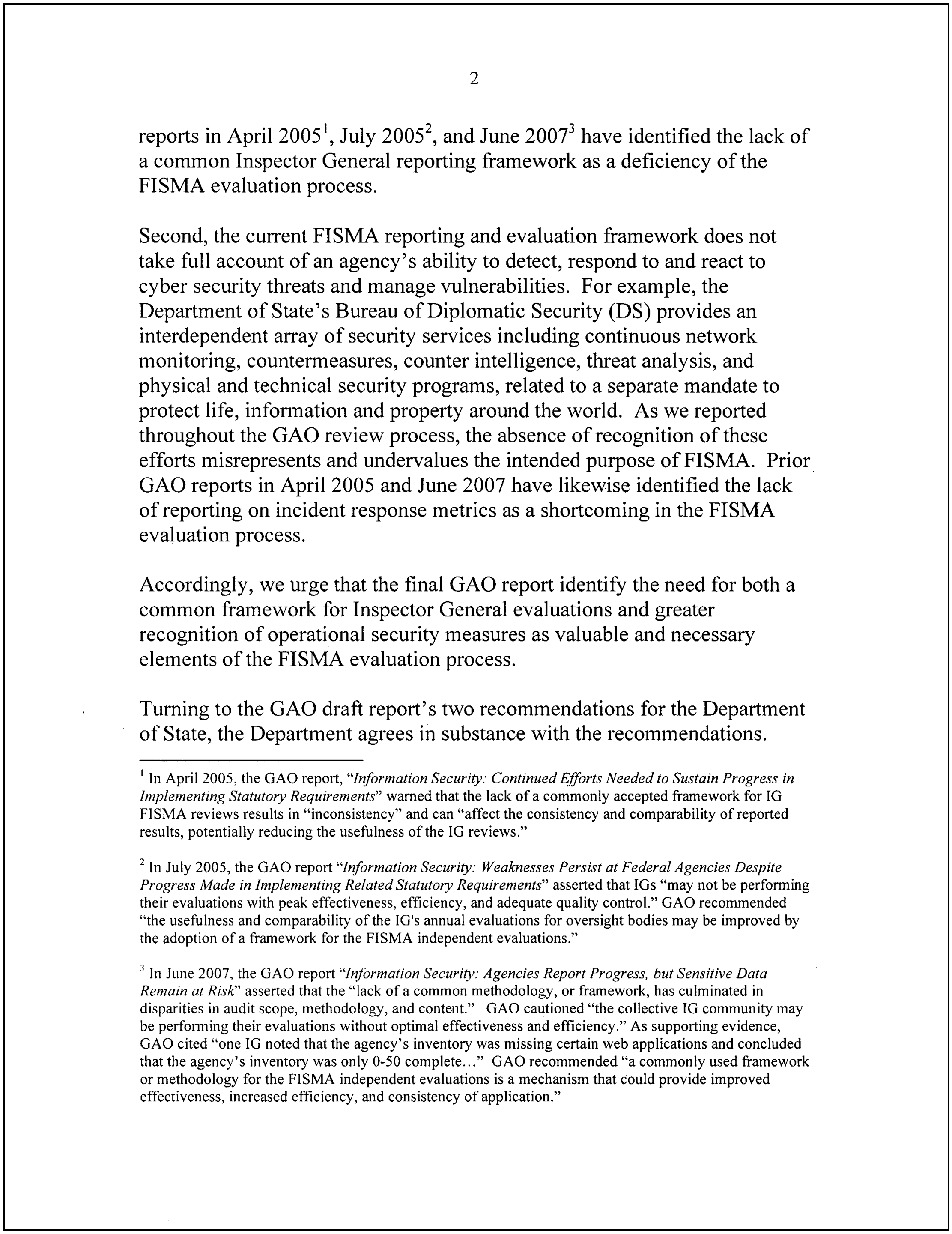
Thank you for the opportunity to review the draft report "*Information Security: Selected Agencies Need to Address challenges in Implementing Statutory Requirements*." In this draft report, the Government Accountability Office's (GAO) objective was to determine the challenges or obstacles that inhibit the implementation of the information security provisions of FISMA at the Departments of Defense, Homeland Security, Justice and State.

GAO's draft report includes two recommendations for the Department of State regarding mechanisms for tracking security awareness training and reported weakness associated with security control testing policies.

As explained below, the Department agrees with the substance of GAO's recommendations and is in the process of effectively addressing them. We would note, however, the Department does not agree with the report's implication that the issues associated with the recommendations serve as challenges or obstacles that inhibit the implementation of the information security provisions of FISMA. Rather, we characterize these to be weaknesses, which merit and are receiving the proper attention.

As an initial matter, the Department would like to highlight two particular areas not currently identified in the draft GAO report, but that have been identified in previous applicable GAO reports and findings. We believe these two areas are significant challenges or obstacles inhibiting the Department from implementing the information security provisions of FISMA, and respectfully request they be included in the final report.

First, the absence of a common/standardized Inspector General reporting framework hinders the Department in its efforts to implement FISMA requirements. As we reported on numerous occasions throughout the GAO review, we find the lack of a common framework for the IG's annual reviews an obstacle because of inconsistent interpretations. Prior GAO



reports in April 2005[1], July 2005[2], and June 2007[3] have identified the lack of a common Inspector General reporting framework as a deficiency of the FISMA evaluation process.

Second, the current FISMA reporting and evaluation framework does not take full account of an agency's ability to detect, respond to and react to cyber security threats and manage vulnerabilities. For example, the Department of State's Bureau of Diplomatic Security (DS) provides an interdependent array of security services including continuous network monitoring, countermeasures, counter intelligence, threat analysis, and physical and technical security programs, related to a separate mandate to protect life, information and property around the world. As we reported throughout the GAO review process, the absence of recognition of these efforts misrepresents and undervalues the intended purpose of FISMA. Prior GAO reports in April 2005 and June 2007 have likewise identified the lack of reporting on incident response metrics as a shortcoming in the FISMA evaluation process.

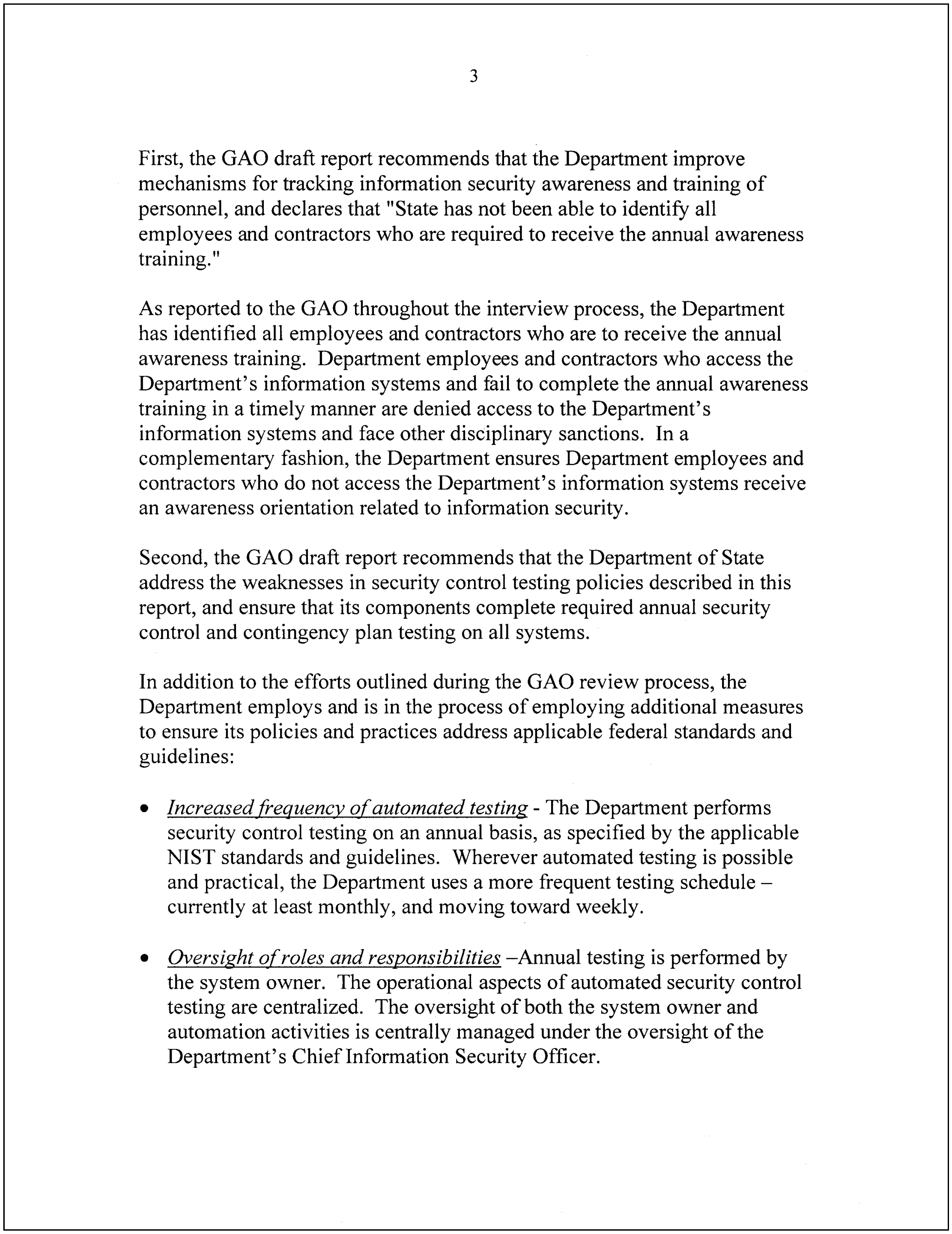
Accordingly, we urge that the final GAO report identify the need for both a common framework for Inspector General evaluations and greater recognition of operational security measures as valuable and necessary elements of the FISMA evaluation process.

Turning to the GAO draft report's two recommendations for the Department of State, the Department agrees in substance with the recommendations.

[1] In April 2005, the GAO report, "*Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements*" warned that the lack of a commonly accepted framework for IG FISMA reviews results in "inconsistency" and can "affect the consistency and comparability of reported results, potentially reducing the usefulness of the IG reviews."

[2] In July 2005, the GAO report "*Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*" asserted that IGs "may not be performing their evaluations with peak effectiveness, efficiency, and adequate quality control." GAO recommended "the usefulness and comparability of the IG's annual evaluations for oversight bodies may be improved by the adoption of a framework for the FISMA independent evaluations."

[3] In June 2007, the GAO report "*Information Security: Agencies Report Progress, but Sensitive Data Remain at Risk*" asserted that the "lack of a common methodology, or framework, has culminated in disparities in audit scope, methodology, and content." GAO cautioned "the collective IG community may be performing their evaluations without optimal effectiveness and efficiency." As supporting evidence, GAO cited "one IG noted that the agency's inventory was missing certain web applications and concluded that the agency's inventory was only 0-50 complete…" GAO recommended "a commonly used framework or methodology for the FISMA independent evaluations is a mechanism that could provide improved effectiveness, increased efficiency, and consistency of application."



First, the GAO draft report recommends that the Department improve mechanisms for tracking information security awareness and training of personnel, and declares that "State has not been able to identify all employees and contractors who are required to receive the annual awareness training."

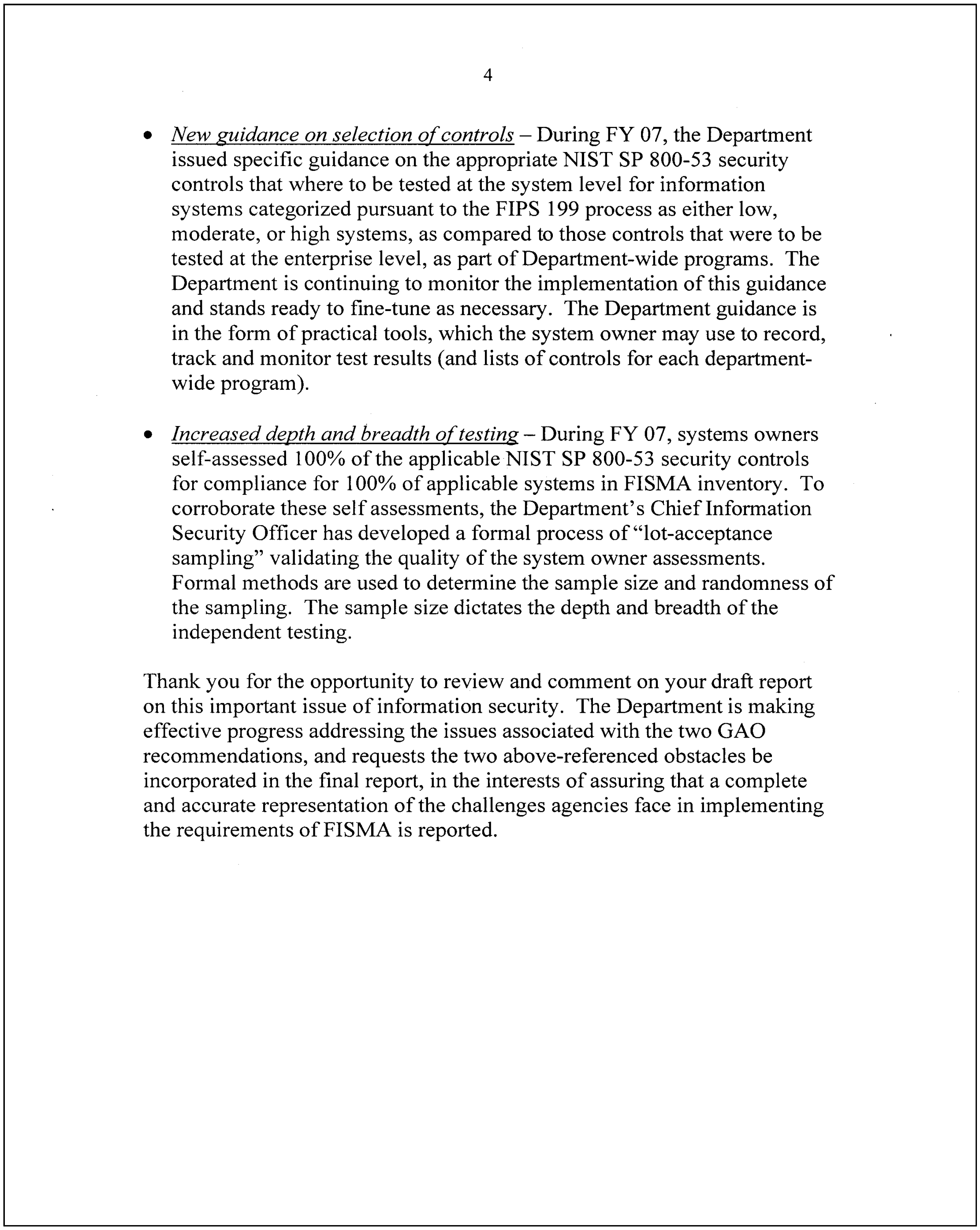
As reported to the GAO throughout the interview process, the Department has identified all employees and contractors who are to receive the annual awareness training. Department employees and contractors who access the Department's information systems and fail to complete the annual awareness training in a timely manner are denied access to the Department's information systems and face other disciplinary sanctions. In a complementary fashion, the Department ensures Department employees and contractors who do not access the Department's information systems receive an awareness orientation related to information security.

Second, the GAO draft report recommends that the Department of State address the weaknesses in security control testing policies described in this report, and ensure that its components complete required annual security control and contingency plan testing on all systems.

In addition to the efforts outlined during the GAO review process, the Department employs and is in the process of employing additional measures to ensure its policies and practices address applicable federal standards and guidelines:

- *Increased frequency of automated testing* - The Department performs security control testing on an annual basis, as specified by the applicable NIST standards and guidelines. Wherever automated testing is possible and practical, the Department uses a more frequent testing schedule – currently at least monthly, and moving toward weekly.

- *Oversight of roles and responsibilities* –Annual testing is performed by the system owner. The operational aspects of automated security control testing are centralized. The oversight of both the system owner and automation activities is centrally managed under the oversight of the Department's Chief Information Security Officer.



- *New guidance on selection of controls* – During FY 07, the Department issued specific guidance on the appropriate NIST SP 800-53 security controls that where to be tested at the system level for information systems categorized pursuant to the FIPS 199 process as either low, moderate, or high systems, as compared to those controls that were to be tested at the enterprise level, as part of Department-wide programs. The Department is continuing to monitor the implementation of this guidance and stands ready to fine-tune as necessary. The Department guidance is in the form of practical tools, which the system owner may use to record, track and monitor test results (and lists of controls for each department-wide program).

- *Increased depth and breadth of testing* – During FY 07, systems owners self-assessed 100% of the applicable NIST SP 800-53 security controls for compliance for 100% of applicable systems in FISMA inventory. To corroborate these self assessments, the Department's Chief Information Security Officer has developed a formal process of "lot-acceptance sampling" validating the quality of the system owner assessments. Formal methods are used to determine the sample size and randomness of the sampling. The sample size dictates the depth and breadth of the independent testing.

Thank you for the opportunity to review and comment on your draft report on this important issue of information security. The Department is making effective progress addressing the issues associated with the two GAO recommendations, and requests the two above-referenced obstacles be incorporated in the final report, in the interests of assuring that a complete and accurate representation of the challenges agencies face in implementing the requirements of FISMA is reported.

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contact named above, key contributions to this report were made by Barbara Collier, Nancy DeFrancesco (Assistant Director), Neil Doherty, Timothy Eagle, Jennifer Franks, Nancy Glover, Anjalique Lawrence, Stephanie Lee, David Plocher, and Jonathan Ticehurst.

(310578)

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

Susan Becker, Acting Manager, Beckers@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON ♻ RECYCLED PAPER