United States Government Accountability Office

GAO

Report to the Ranking Minority Member,
Committee on Homeland Security and
Governmental Affairs, U.S. Senate

June 2005

INFORMATION SECURITY

Department of Homeland Security Needs to Fully Implement Its Security Program

Accountability ★ Integrity ★ Reliability

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-05-700, a report to the Ranking Minority Member, Committee on Homeland Security and Governmental Affairs, U.S. Senate

June 2005

INFORMATION SECURITY

Department of Homeland Security Needs to Fully Implement Its Security Program

Why GAO Did This Study

The Homeland Security Act of 2002 mandated the merging of 22 federal agencies and organizations to create the Department of Homeland Security (DHS), whose mission, in part, is to protect our homeland from threats and attacks. DHS relies on a variety of computerized information systems to support its operations. GAO was asked to review DHS's information security program. In response, GAO determined whether DHS had developed, documented, and implemented a comprehensive, departmentwide information security program.

What GAO Recommends

To assist DHS in fully implementing its program, GAO is making recommendations to the Secretary of DHS to implement key information security practices and controls and to establish milestones for verifying the department's reported performance data. In providing written comments on a draft of this report, DHS generally agreed with the contents of the report and described actions recently completed, ongoing, or planned to implement its program.

www.gao.gov/cgi-bin/getrpt?GAO-05-700.

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

What GAO Found

DHS has not fully implemented a comprehensive, departmentwide information security program to protect the information and information systems that support its operations and assets. It has developed and documented departmental policies and procedures that could provide a framework for implementing such a program; however, certain departmental components have not yet fully implemented key information security practices and controls. For example, risk assessments—needed to determine what controls are necessary and what level of resources should be expended on them—were incomplete. Elements required for information system security plans—which would provide a full understanding of existing and planned information security requirements—were missing. Testing and evaluation of security controls—which are needed to determine the effectiveness of information security policies and procedures—were incomplete or not performed. Elements required for remedial action plans—which would identify the resources needed to correct or mitigate known information security weaknesses—were missing, as were elements required for continuity of operations plans to restore critical systems in case of unexpected events. The table below indicates with an "X" where GAO found weaknesses. In addition, DHS had not yet fully developed a complete and accurate systems inventory.

Weaknesses in Information Security Practices and Controls of Selected DHS Components

DHS component	Risk assessment	Security plan	Security test and evaluation	Remedial action plans	Continuity of operations
US-VISIT	n/a	X[a]	n/a	n/a	n/a
ICE			X	X	X
TSA			X	X	X
ICE	X		X		X
TSA	X		X	X	X
EP&R	X	X		X	X

Sources: GAO analysis of DHS information for United States Visitor and Immigrant Status Indicator Technology (US-VISIT), Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), and Emergency Preparedness and Response (EP&R).

[a] For US-VISIT, GAO reviewed only the security plan.

Shortfalls in executing responsibilities for ensuring compliance with the information security program allowed these weaknesses to occur. Although DHS has an organization that is responsible for overseeing the component implementation of key information security practices and controls, its primary means for doing so—an enterprisewide tool—has not been reliable. Until DHS addresses weaknesses with using the tool and implements a comprehensive, departmentwide information security program, its ability to protect its information and information systems will be limited.

United States Government Accountability Office

Contents

Letter

Appendixes

Table

Figure

Abbreviations

CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

G A O

Accountability ★ Integrity ★ Reliability

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

June 17, 2005

The Honorable Joseph I. Lieberman
Ranking Minority Member
Committee on Homeland Security and Governmental Affairs
United States Senate

Dear Senator Lieberman:

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.

Responding to current and potential threats to homeland security is one of the federal government's most significant challenges. To address this challenge, the Homeland Security Act of 2002 (Pub. L. No. 107-296) mandated the merger of 22 federal agencies and organizations with homeland security-related missions to create the Department of Homeland Security (DHS). Since it became operational in March 2003, DHS has not only faced the challenge of protecting the homeland, but also with transforming this collection of diverse entities into a single new cabinet-level department. In order to meet this challenge, it is crucial that DHS establish an effective information security program to protect the information and information systems that support its operations and assets.

In response to your request, our objective was to determine whether DHS had developed, documented, and implemented a comprehensive, departmentwide information security program. To accomplish this objective, we reviewed pertinent information security policies, procedures and practices in place at the department and its component organizations from information system security managers and other key officials. Our review of DHS's information security program was based in part, on the

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

requirements of the Federal Information Security Management Act of 2002 (FISMA)[2] and relevant Office of Management and Budget (OMB) policies[3] and National Institute of Standards and Technology (NIST) guidance related to performing risk assessments, developing information security plans, testing and evaluating security controls, documenting remedial action plans, and documenting and testing continuity of operations plans. Details on our scope and methodology are included in appendix I.

We performed our review at DHS facilities in the Washington, D.C., metropolitan area, Denver, Colorado, and at our headquarters in Washington, D.C., from July 2004 through May 2005, in accordance with generally accepted government auditing standards.

Results in Brief

DHS has not fully effectively implemented a comprehensive, departmentwide information security program to protect the information and information systems that support its operations and assets. It has developed and documented departmental policies and procedures that could provide a framework for implementing a departmentwide information security program; however, certain departmental components have not yet fully implemented key information security practices and controls. For example, components' weaknesses in implementing the program included incomplete risk assessments for determining the required controls and the level of resources that should be expended on them; missing required elements from information system security plans for providing a full understanding of the existing and planned information security requirements; incomplete or nonexistent test and evaluation of security controls for determining the effectiveness of information security policies and procedures; missing required elements from remedial action plans for identifying the resources needed to correct or mitigate identified information security weaknesses; and incomplete, nonexistent or untested continuity of operations plans for restoring critical systems in the case of unexpected events. In addition, DHS had not yet fully developed a complete and accurate systems inventory.

[2] *Federal Information Security Management Act of 2002*, *Title III*, *E-Government Act of 2002*, Pub. L. No. 107-347, Dec.17, 2002.

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

Shortfalls in executing the responsibilities for ensuring compliance with the departmentwide information security program allowed the weaknesses that we identified to occur. Although the Chief Information Security Officer (CISO) has responsibility for overseeing DHS components' compliance with key information security practices and controls, the primary means for doing so—an enterprise management tool known as Trusted Agent FISMA—has not been reliable. The DHS Office of the Inspector General (OIG) identified weaknesses with this tool that make it unreliable for use in overseeing the components' reported performance data on their compliance with key information security activities. Specifically, the OIG reported that the data are not comprehensively verified, there is no audit trail capability, material weaknesses are not consistently reported or linked to plans of actions and milestones, and plans of actions and milestones that have been identified and documented are not current. Until DHS addresses these weaknesses and fully implements a comprehensive, departmentwide information security program, its ability to protect the confidentiality, integrity and availability of its information and information systems will be limited.

To assist DHS in fully implementing its program, we are making recommendations to the Secretary of DHS to fully implement key information security practices and controls and to establish milestones for developing a comprehensive information systems inventory and for verifying the department's reported performance data. In providing written comments on a draft of this report, DHS generally agreed with the contents of the report and described actions to implement its security program.

Background

To address the challenge of responding to current and potential threats to homeland security—one of the federal government's most significant challenges—Congress passed, and the President signed, the Homeland Security Act of 2002.[4] This act mandated the merger of 22 federal agencies and organizations into DHS. Not since the creation of the Department of Defense in 1947 has the federal government undertaken a transformation of this magnitude. In March 2003, DHS assumed operational control of about 209,000 civilian and military positions from these 22 federal agencies and organizations. Each of these agencies and organizations brought with it management challenges, distinct missions, unique information technology

[4] Public Law 107-296 (November 25, 2002).

infrastructures and systems, and its own policies and procedures. Because of the importance of the department's operations and the challenges associated with creating the federal government's third largest department, we designated the implementation and transformation of DHS as a high-risk area in January 2003.[5]

Department of Homeland Security's Mission and Organization

DHS's mission, in part, is to prevent and deter terrorist attacks within the United States,[6] reduce the vulnerability of the United States to terrorism, and to minimize the damage, and assist in the recovery, from terrorist attacks that do occur.[7] This is an exceedingly complex mission that requires coordinated and focused effort from the federal government, state and local governments, the private sector, and the American people. The Department of Homeland Security Appropriations Act of 2005,[8] provided $28.9 billion in net discretionary spending for DHS to carry out its mission.

To accomplish its mission, the Homeland Security Act of 2002 established five under secretaries with responsibilities over directorates for management, science and technology, information analysis and infrastructure protection, border and transportation security, and emergency preparedness.[9] Each directorate is responsible for its specific homeland security mission area. DHS aligned the 22 federal agencies and

[5] GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

[6] 6 U.S.C. § 113(a).

[7] 6 U.S.C. § 111(b).

[8] Pub. L. No. 108-334 (Oct. 18, 2004).

[9] 6 U.S.C. § 113(a).

organizations into 13 major agency components[10] (see fig. 1). The 13 components and their missions:

- *Office of Management*—responsible for such things as the budget, appropriations, expenditure of funds, accounting and finance, procurement, and information technology.

- *Science and Technology*—serve as the primary research and development arm of DHS with a focus on catastrophic terrorism—threats to the security of our homeland that could result in large-scale loss of life and major economic impact.

- *Transportation Security Administration*—protect the nation's transportation systems by ensuring the freedom of movement for people and commerce.

- *Customs and Border Protection*—manage, control, and protect the nation's borders at and between the official ports of entry.

- *Immigration and Customs Enforcement*—prevent acts of terrorism by targeting the people, money, and materials that support terrorist and criminal activities. It is the largest investigative arm of DHS.

- *Federal Law Enforcement Training Center*—prepare federal, state, local, and international law enforcement professionals to fulfill their responsibilities safely and proficiently, ensuring that training is accomplished in the most cost-effective manner.

- *Emergency Preparedness and Response*—ensure that our nation is prepared for incidents—whether natural disasters or terrorist assaults—and oversees the federal government's national response and recovery strategy.

[10] DHS aggregates the 13 major agency components' data and reports on the department's compliance with the Federal Information Security Management Act of 2002 (FISMA). However, as shown in figure 1, the Transportation Security Administration, Customs and Border Protection, Immigration and Customs Enforcement, and Federal Law Enforcement Training Center report to the Under Secretary Border and Transportation Security; and the Under Secretary Border and Transportation Security is not a separate component for FISMA reporting.

- *Information Analysis and Infrastructure Protection*—help deter, prevent, and mitigate acts of terrorism by assessing vulnerabilities in the context of continuously changing threats.

- *Citizen and Immigration Services*—promote national security, eliminate immigration case backlogs, improves customer services, and provide administrative services such as immigrant and nonimmigrant sponsorship, work authorization and other permits, and naturalization of qualified applicants for U.S. citizenship.

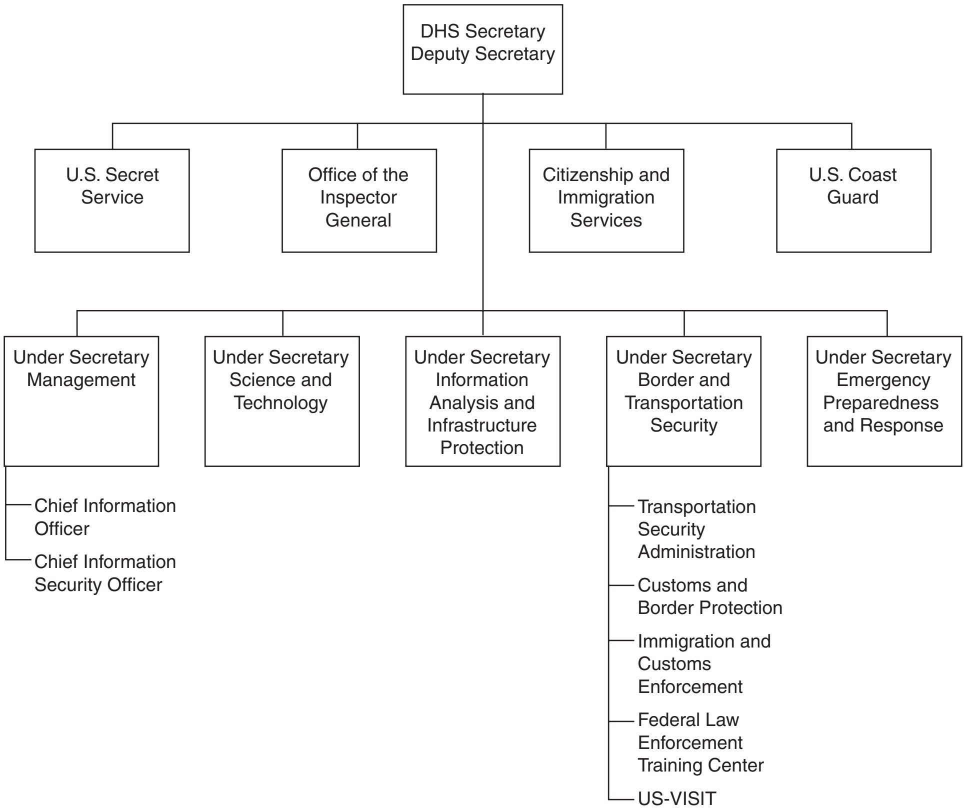
- *Office of the Inspector General (OIG)*—serve as an independent and objective inspection, audit, and investigative body to promote effectiveness, efficiency, and economy in the DHS's programs and operations, and to prevent and detect fraud, abuse, mismanagement, and waste in such programs and operations.

- *U.S. Coast Guard*—protect the public, the environment, and U.S. economic interests in the nation's ports and waterways, along the coast, on international waters, or in any maritime region, as required to support national security.

- *U.S. Secret Service*—protect the President and our nation's leaders, as well as our country's financial and critical infrastructures.

- *United States Visitor and Immigrant Status Indicator Technology (US-VISIT)*— a DHS program intended to collect, maintain, and share information on foreign nationals through Immigration and Customs Enforcement and Customs and Border Protection systems in order to expedite the arrival and departure of legitimate travelers, while making it more difficult for those intending to do harm to our nation.

Figure 1: Overview of the Department of Homeland Security's Organizational Structure


DHS Secretary
Deputy Secretary
U.S. Secret Service
Office of the Inspector General
Citizenship and Immigration Services
U.S. Coast Guard
Under Secretary Management
Under Secretary Science and Technology
Under Secretary Information Analysis and Infrastructure Protection
Under Secretary Border and Transportation Security
Under Secretary Emergency Preparedness and Response
Chief Information Officer
Chief Information Security Officer
Transportation Security Administration
Customs and Border Protection
Immigration and Customs Enforcement
Federal Law Enforcement Training Center
US-VISIT

Source: GAO analysis of DHS organizational structure.

Within the Office of the Under Secretary Management is the Office of the Chief Information Officer (CIO). Under the authorities of the Clinger-Cohen Act of 1996,[11] FISMA, and DHS management directives, the DHS CIO is responsible for ensuring compliance with federal information security requirements and reporting annually to the DHS Secretary on the effectiveness of the department's information security program. The CIO designated the CISO, under the authorities of FISMA,[12] to carry out specific information security responsibilities that include

[11] 40 U.S.C. § 11315.

[12] 44 U.S.C. § 3544 (a)(3).

- developing and maintaining a departmentwide information security program, as required by FISMA;

- developing departmental information security policies and procedures to address the requirements of FISMA;

- providing the direction and guidance necessary to ensure that information security throughout the department is compliant with federal information security requirements and policies; and

- advising the CIO on the status and issues involving security aspects of the departmentwide information security program.

In addition, the CISO is responsible for oversight functions such as those required to ensure that DHS has departmentwide, repeatable, and robust processes for meeting federal information security requirements and that the components accurately assess their security postures.

Information system security managers at each of the components are expected to assist the CISO in carrying out its oversight functions. Security managers have the role of maintaining the confidentiality, integrity, and availability of the DHS programs and systems that support the department's missions and operations. They are responsible for providing the link between the departmentwide information security program and the components. Security managers are also responsible for ensuring that the information system security officers and program officials at their respective components are in compliance with federal information security requirements and policies.

Information system security officers serve as the focal point for information security activities at the system level in each DHS component. Among other things, security officers have the responsibility for ensuring that appropriate steps are taken to implement information security requirements for information systems throughout their life cycle. Security managers directly report to the CIO at their respective component and security officers directly report to their program officials, who directly report to their respective component heads. Program officials are required to implement information security controls and manage risk for information assets pertaining to their business need.

DHS Uses a Variety of Systems to Support Its Mission Operations

The department uses a variety of major applications and general support systems to support its operations. A major application is one that requires special attention due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications and people and can be, for example, a local area network or communications network.

Many of these applications and systems serve specific requirements unique to individual component's missions and result in interoperability issues, data management concerns, and incompatible environments or duplicative/inefficient processes. As noted in DHS's March 2004 *Information Resource Management Strategic Plan*, DHS's CIO has established the goal of forming one network and one information technology infrastructure to facilitate information sharing within the department and among DHS and external federal, state, and local agencies.

Information Security is Critical for Agencies to Effectively Accomplish Their Missions

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. 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. Without proper safeguards, they also pose enormous risks that make it easier for individuals and groups with malicious intent to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

Protecting the computer systems that support critical operations and infrastructures has never been more important because of the concern about attacks from individuals and groups, including terrorists. These concerns are well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technologies, and the dire warnings of new and more destructive attacks to come.

Computer-supported federal operations are likewise at risk. Our previous reports,[13] and those of agency inspectors general, describe persistent information security weaknesses that place a variety of critical federal operations, including DHS, at risk of disruption, fraud, and inappropriate disclosure.

FISMA Authorized and Strengthened 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. FISMA assigns specific responsibilities to agency heads, chief information officers, and Inspectors General (IG). It assigns responsibilities to the OMB as well; these include developing and overseeing the implementation of policies, principles, standards, and guidelines for information security; reviewing agency information security programs at least annually; and approving or disapproving these programs.

FISMA requires each agency to develop, document, and implement a departmentwide information security program. This program should establish security measures for the information and information systems that support the operations and assets of the agency—including those provided or managed by another agency, a contractor, or another source. This program is to include

- 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;
- 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;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;

[13] See, for example, GAO-05-207; DHS, OIG, *DHS Needs to Strengthen Controls For Remote Access to Its Systems and Data*, OIG-05-03 (November 2004); GAO, *Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk*, GAO-05-362 (Washington, D.C.; April 2005); and DHS, OIG, *Inadequate Security Controls Increase Risks to DHS Wireless Networks*, OIG-04-27 (June 2004).

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

- a process for planning, implementing, evaluating, and documenting remedial actions that are taken to address any deficiencies in the agency's information security policies, procedures, and practices; and

- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

FISMA also establishes a requirement that each agency develops, maintains, and annually updates an inventory of major information systems that the agency operates or that are under its control. Among other things, this inventory is to identify the interfaces between each system and all other systems or networks with which it communicates, including those that are not operated by, or under the control of, the agency.

Each agency is also required to undergo an annual, independent evaluation of its information security program and practices, including control testing and compliance assessment. Evaluations of nonnational security systems are to be performed by the agency's IG or by an independent external auditor; evaluations related to national security systems are to be performed only by an entity designated by the agency head. Agencies are to report annually to OMB on the results of their independent evaluations. OMB then summarizes the results of the evaluations in a report to selected congressional committees.

Other major provisions require NIST to develop, for systems other than national security systems, (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 to be included in each category, and (3) minimum information security requirements for information and information systems in each category. NIST must also develop (1) a definition of and guidelines concerning the detection and handling of information security incidents and (2) guidelines developed in coordination with the National Security Agency for identifying an information system as a national security system.

DHS Has Developed and Documented an Information Security Program, but Weaknesses in Implementation Remain

Since DHS became operational in March 2003, the CISO has developed and documented departmental policies and procedures that could provide a framework for implementing an agencywide information security program; however, certain DHS components had not yet fully implemented key information security practices and controls, as required by the program. The CISO has taken several actions to develop and document a departmentwide information security program. These actions include

- development, documentation, and dissemination of DHS information security policies and procedures, strategic program plans, risk management plans, and a management directive and handbook for the components' use in implementing the requirements of the program;
- establishment of Information System Security Managers and Information System Security Officers positions to implement DHS's information security program departmentwide;
- documentation and issuance of specific guides to assist security managers and security officers in aligning their individual components' information security programs with the department's program;
- development of Trusted Agent FISMA and a digital dashboard as tools to aggregate and report component and department level data for enterprise management and oversight of the departmentwide information security program; Trusted Agent FISMA is an enterprise compliance and oversight tool that manages the collection and reporting of the components' information associated with key information security practices and controls, and the digital dashboard aggregates the data collected in Trusted Agent FISMA and is used as a visual tool using a traffic light display to gauge the progress of the departmentwide information security program; and
- development and documentation of a departmentwide systems inventory methodology that is designed to be used to develop, maintain, and annually update an inventory of information systems operated by the department or under its control.

In addition, as part of the department's efforts to develop and document a departmentwide information security program, the CISO finalized the *Information Security Program Strategic Plan* in April 2004, which provides a framework for establishing a unified, departmentwide information security program.

Implementation Weaknesses Place DHS's Operations and Assets at Risk

Although the CISO has made significant progress in developing and documenting a departmentwide information security program, certain DHS components have not yet fully implemented key information security practices and controls as required by the program. We identified weaknesses in information security documentation for the three major applications and three general support systems that we selected for review that place DHS's operations and assets at risk. Among other things, DHS's program requires the components to maintain information security documentation in accordance with FISMA requirements, OMB policies, and applicable NIST guidance. However, we identified that risk assessments were not complete, security plans lacked required elements, test and evaluation of security controls were either not comprehensive or not performed, plans of action and milestones lacked required elements, and continuity of operations plans were not complete, lacked required elements, or had not been tested. In addition, DHS had not yet fully developed a complete and accurate information systems inventory. As a result of these weaknesses, DHS's ability to protect the confidentiality, integrity, and availability of its information and information systems was limited.

Table 1 indicates with an "X" where we found weaknesses in selected components' information security practices and controls.

Table 1: Weaknesses in DHS Selected Components' Information Security Practices and Controls

DHS System	DHS component	Risk assessment	Security plan	Security test and evaluation	Remedial action plans	Continuity of operations
Major application	US-VISIT	n/a	X[a]	n/a	n/a	n/a
Major application	ICE			X	X	X
Major application	TSA			X	X	X
General support system	ICE	X		X		X
General support system	TSA	X		X	X	X
General support system	EP&R	X	X		X	X

Source: GAO analysis of information security documentation for United States and Immigrant Status Indicator Technology (US-VISIT), Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), and Emergency Preparedness and Response (EP&R) systems.

[a] For each system, we obtained and reviewed all documentation contained in the certification and accreditation package—with the exception of US-VISIT—in this case, we reviewed only the security plan.

Risk Assessments

Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls. Moreover, by increasing awareness of risks, these assessments generate support for the policies and controls that have been adopted, which helps ensure that these policies and controls operate as intended. FISMA requires agency's information security programs to 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.

Risk assessments for three of the five systems were not complete. For example, two general support systems—one at Transportation Security Administration and one at Immigration and Customs Enforcement—had risk assessment reports that were in draft and incomplete. In addition to the weaknesses we identified, the OIG, as part of its fiscal year 2004 FISMA evaluation, identified that risk assessments for selected DHS systems that they reviewed were not current. Unless DHS performs periodic risk assessments of its information systems, it will not have assurance that appropriate controls over potential threats have been identified to reduce or eliminate the associated risk.

Security Plans

The purpose of an information system security plan is to provide an overview of the security requirements of the system and describe the controls that are in place or planned for meeting those requirements. The information security plan also delineates the responsibilities and expected behavior of all individuals who access the system. The information security plan can be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system and should form the basis for the system authorization, supplemented by more specific studies as needed. According to NIST guidance, security plans should include all interconnected systems (including the Internet) and interaction among systems in regard to the authorization for the connection to other systems or the sharing of information. Also according to NIST guidance, security plans should include rules of behavior and reflect input from various individuals who have responsibility for the system, including information system owners. In addition, the security plans require periodic reviews, modifications, and milestone or completion dates for planned controls.

The information security plans for two of the six systems we reviewed lacked required elements. Specifically, the information security plan for a US-VISIT major application did not include authorizations for interconnected systems or the sharing of information for primary and secondary systems and for other infrastructures. In addition, the Internet was not included in the list of interconnected systems. Further, rules of behavior, another required element for security plans, did not cover all pertinent elements such as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability. The information security plan for the general support system at the Emergency Preparedness and Response directorate did not identify a designated information system owner or procedures for reviewing the information security plan and following up on planned controls. The OIG, as part of its fiscal year 2004 FISMA evaluation, found that security plans for the DHS systems that it had selected for review had either not been updated or not approved. As a result of these weaknesses, DHS does not have assurance that its information systems are adequately protected.

Testing and Evaluation

Another key element of an information security program is periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices. FISMA requires that the frequency with which an organization should conduct testing and evaluation will depend on the level of risk. This testing and evaluation should be conducted at least annually and include testing of management, operational, and technical controls of every system identified in the agency's information systems inventory. Management control testing, for example, includes integration testing, which occurs in the program's actual operating environment and tests such things as connectivity with other systems and networks. Periodically testing and evaluating the effectiveness of security policies and controls is a fundamental activity that allows an agency to manage its information security risks cost-effectively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported. Such testing and evaluation helps provide a more complete picture of agencies' security postures.

DHS did not fully test and evaluate the security controls of four of the five major systems we reviewed. For example, the Transportation Security Administration did not test and evaluate security controls and policies for a major application and general support system. Further, Immigration and Customs Enforcement did not have final test and evaluation reports for a major application and general support system. Although we did not obtain the test and evaluation report for US-VISIT, the information security plan identified that comprehensive testing had not occurred for one major application. Specifically, the application owner did not conduct systems integration testing in the program's actual operating environment to test such things as connectivity with other systems and networks. In its fiscal year 2004 FISMA report, DHS identified that 24 percent of its systems had not undergone test and evaluation. Without adequately testing and evaluating systems, the department cannot be assured that security controls are in place and functioning correctly to protect its information and information systems.

Remedial Action Plans

FISMA requires each agency to develop a process for planning, implementing, evaluating, and documenting remedial action plans, referred to as plans of action and milestones by OMB, to address any deficiencies in the information security policies, procedures, and practices. The CIO is to manage the process for the agencies and be regularly updated by program officials on their progress in implementing remedial actions. This process allows both the CIO and the OIG to monitor departmentwide progress, identify problems, and provide accurate reporting. In its guidance for annual reporting, OMB asks the agency IGs to report on the status of the plans of action and milestones at their agencies. IGs were asked to evaluate the process based on several criteria, including whether systems plans are tied directly to the system budget request through the information technology business case, as required by OMB.

For four of the five systems that we reviewed, program officials either did not identify any resources in their plans of action and milestones submissions, as required by OMB, to correct or mitigate identified information security weaknesses or had not prepared plans of action and milestones. As part of its fiscal year 2004 FISMA evaluation, the OIG reported that DHS's plans of action and milestones process was not adequate. Specifically, the estimated funding necessary to correct or mitigate information security weaknesses was not identified in the components' plans of action and milestones submissions, system-level plans of action and milestones were not linked to individual components' budget submissions, and not all of the components were capturing information security weaknesses from all sources for reporting on their plans of action and milestones. We found that a major application at Immigration and Customs Enforcement and a general support system at Emergency Preparedness and Response had not allocated any funds to correct specifically identified weaknesses. Although some actions did not have an associated cost, there were instances where it was apparent that costs would be incurred for the corrective action. Further, the Transportation Security Administration did not prepare plans of action and milestones for information security weaknesses associated with a major application and general support system. As a result, DHS does not have assurance that all information security weaknesses have been reported and that corrective actions will appropriately be taken to address the weaknesses.

Continuity of Operations

Continuity of operations plans provide specific instructions for restoring critical systems, including such elements as arrangement for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed due to unexpected events. These events may include such things as temporary power failure, accidental loss of files, or a major disaster. It is important that these plans be clearly documented, communicated to potentially affected staff, and updated to reflect current operations. According to NIST guidance, continuity planning includes establishing thorough plans, procedures, and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster. Further, the testing of continuity of operations plans is essential to determining whether plans will function as intended in an emergency situation.

For all five of the continuity of operations plans reviewed, program officials either did not include all information necessary to restore operations in the event of a disaster or have a documented plan. For example, the continuity of operations plans for an Immigration and Customs Enforcement general support system and a major application lacked critical information such as the activities necessary to return to normal operations, personnel contact information, locations of associated telecommunications infrastructure, location of off-site storage for backup media, and vendor contact information. Further, program officials did not have continuity of operations plans for a Transportation Security Administration major application and general support system. The OIG also reported deficiencies in DHS's continuity of operations plans. Specifically, the OIG performed a quality review of selected certification and accreditation packages and found instances where continuity of operations plans did not meet all of the applicable requirements. Further, the OIG identified instances in which systems were accredited even though continuity of operations plans had not been developed or tested. Moreover, in its FISMA report to OMB for fiscal year 2004, DHS had reported that 79 percent of its systems did not have a tested continuity of operations plan. As a result, the department has limited assurance that it will be able to protect its critical and sensitive information and information systems and resume operations promptly when unexpected events or unplanned interruptions occur.

DHS Does Not Have a Complete and Accurate Information Systems Inventory

FISMA requires agencies to develop, maintain, and annually update an inventory of information systems that are either operated by the agency or under its control. The inventory is to identify the interfaces between each system and all the other systems or networks with which it communicates, including those that are not operated by or under the control of DHS.

In December 2004, the DHS CISO approved a departmentwide information systems inventory methodology that its contractor developed and has begun implementing it across the department. Our assessment of the methodology determined that it is appropriately based on the requirements of FISMA, OMB policies, and applicable NIST guidance and standards and, if fully implemented, could provide the department with a comprehensive inventory of its information systems.

As of March 2005, DHS has completed the information systems inventory for the OIG and the Transportation Security Administration and is completing its efforts to implement the methodology at the Immigration and Customs Enforcement. In response to the OIG's fiscal year 2004 FISMA report, which reiterated its prior year recommendation that DHS develop a complete and accurate systems inventory, DHS acknowledged that it needs a complete and accurate systems inventory for all of its components in order to effectively manage its program and ensure departmentwide implementation. Subsequent to that report, DHS established a milestone of August 5, 2005, for developing a complete DHS systems inventory. Until DHS has a complete and accurate systems inventory, DHS will be inhibited in its ability to oversee and manage the information and information systems that support the operations and assets of the agency.

Management Oversight Needs Improvement

Shortfalls in executing the responsibilities for ensuring compliance with the departmentwide information security program allowed the weaknesses that we identified to occur. The CISO has responsibility for overseeing DHS components' compliance with key information security practices and controls. To fulfill this responsibility, the CISO developed and implemented Trusted Agent FISMA[14] in order to aggregate the component's reported performance data that arise from annual self-assessments and OMB metrics for key information security activities, such as number of significant deficiencies and whether remedial action plans to address the deficiencies had been developed, and the number of system continuity of operations plans documented and tested. Security officers at the components are responsible for updating the tool with data that arise from annual self-assessments, as well as from other system-level security metrics. The security managers have the responsibility for ensuring that all required metrics data are updated. These data are aggregated in the digital dashboard[15] and reported to OMB for the department as a whole.

[14] Trusted Agent FISMA is an enterprise tool for aggregating data reported by the components to gauge how well the department is complying with key information security practices and controls.

[15] The digital dashboard is to serve as a management tool to ensure the components take a risk-based, cost-effective approach to secure their information and information systems, identify and resolve current information security weaknesses and risks, as well as protect against future vulnerabilities and threats. The dashboard allows management to monitor the components' remediation efforts to identify progress and problems. Each component's success in meeting the FISMA requirements is reported as a percentage of compliance, along with a red, amber, or green color-coded gauge or traffic light display.

However, the OIG identified that DHS could not rely on the accuracy and completeness of the data contained in Trusted Agent FISMA, which contributed to the OIG's overall recommendation that DHS continue to consider its information security program a significant deficiency for fiscal year 2004. Examples of the weaknesses that they identified include

- significant weaknesses were not consistently reported or linked to plans of action and milestones;
- plans of action and milestones that have been identified and documented included some that were neither current nor updated periodically;
- some data fields, such as the "Scheduled Completion Date," for plans of action and milestones that could be arbitrarily revised by the components with no audit trail to monitor such activity; and
- information entered by the components was not verified.

Unless the data being collected and tracked from the components are reliable, the CISO has no assurance that the components' metrics accurately reflect the status of their implementation of key information security activities. Having reliable metrics on key activities such as those we identified as having weaknesses—risk assessments, security plans, security test and evaluation, remedial action plans, and continuity of operations plans—is critical. According to DHS's information security policies and procedures, the CISO is to use these metrics to validate the efficacy of the program, identify gaps between reported and actual performance data, and help focus attention on presidential, congressional, or department priorities. In response to the OIG's FISMA evaluation, the CIO stated that the department had recently initiated a project to review and verify the metrics data. However, the CIO has not established a milestone for completing this project. Implementing a process for verifying the reported data could help improve the quality of the information used by the CISO to oversee the components' compliance with the departmentwide information security program.

Conclusions

DHS has not fully implemented a comprehensive, departmentwide information security program, thereby jeopardizing the confidentiality, integrity, and availability of the information and information systems that it relies on to accomplish its mission. DHS's efforts to date in developing and documenting such a program has merit. However, ensuring that the components implement key information security practices and controls, especially with a department as diverse as DHS, requires effective management oversight and monitoring. Having a complete and accurate information systems inventory and a process in place to verify the components' data on their implementation of the key information security practices and controls is needed for DHS to effectively implement its information security program. However, until it does so, DHS will have limited assurance that its operations and assets are adequately protected.

Recommendations for Executive Action

To help fully implement DHS's departmentwide information security program, we recommend that the Secretary of DHS direct the Chief Information Officer to

- instruct the CISO and component agencies to fully implement the following key information security practices and controls by
  - developing complete risk assessments;
  - documenting comprehensive security plans;
  - fully performing testing and evaluation of security controls;
  - reporting complete remedial action plans; and
  - developing, documenting, and testing continuity of operations plans.
- establish milestones for completing verification of the components' reported performance data in Trusted Agent FISMA.

Agency Comments

In providing written comments on a draft of this report, DHS's Chief Information Security Officer generally agreed with the contents of the report and described recently completed, ongoing or planned efforts to implement the department's information security program. For example, the Chief Information Security Officer stated that the agency has efforts under way to improve processes for developing complete risk assessments; documenting and updating security plans; verifying the results of annual testing and evaluation of security controls; reporting complete remedial action plans; and developing, documenting, and testing continuity of operations plans. The Chief Information Security Officer also stated that enhancements have been made to the Trusted Agent FISMA tool in order to improve the reliability of the components' reported performance data. DHS's comments are reprinted in appendix II of this report.

As agreed with your offices, unless you publicly announce its contents earlier, we will not distribute this report further until 30 days from the report date. At that time, we will send copies to interested congressional committees, the DHS Secretary and, upon their request, to other interested parties. In addition, the report will be made available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions about this report, please contact me at (202) 512-6244 or via 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 acknowledged in appendix III.

Sincerely yours,

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I

Scope and Methodology

To determine whether the Department of Homeland Security (DHS) had developed and documented a departmentwide information security program, we reviewed departmental information security plans, policies, procedures, and handbooks; agencywide tools for aggregating the components' performance data on their assessment of meeting the requirements of the Federal Information Security Management Act of 2002 (FISMA); and DHS's information systems inventory methodology. We assessed whether DHS's departmentwide information security program was consistent with the requirements of FISMA and applicable Office of Management and Budget (OMB) policies[1] and NIST guidance related to performing risk assessments, developing information security plans, testing and evaluating security controls, documenting remedial action plans, and documenting and testing continuity of operations plans.

To determine whether DHS had implemented its departmentwide information security program, we focused our review on the components' alignment with key information security practices and controls. To accomplish this, we selected seven DHS components—five of which DHS categorize as major agency components due to their size and mission. The five components selected were: Customs and Border Protection, Transportation Security Administration, Immigration and Customs Enforcement, U.S. Coast Guard, and Emergency Preparedness and Response. We also selected these five components because they had been in existence prior to the transformation of DHS and, from an evaluation standpoint, focused on determining their progress in aligning with and implementing the departmentwide information security program given these components had their own information technology management structures, information security policies and practices, and infrastructures. As a comparison, we selected one component—Science and Technology—that had not existed prior to the transformation to evaluate its alignment with and implementation of the departmentwide information security program. We also selected the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program due to its significant mission in providing security to our nation's borders.

Based on their criticality to DHS's mission operations, we selected for review three major applications and three general support systems and obtained documentation contained in the certification and accreditation

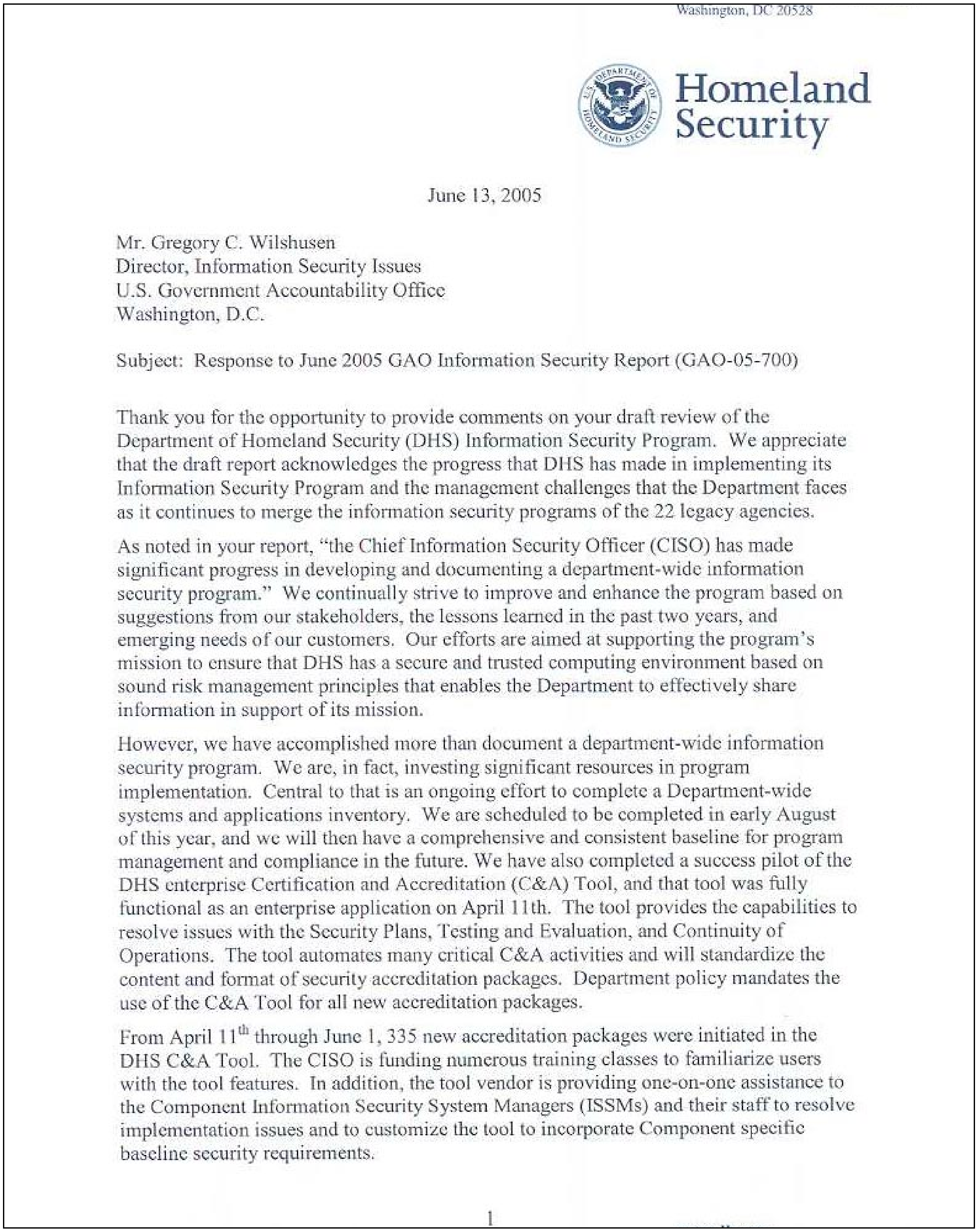
[1] Office of Management and Budget, Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (Washington, D.C.: Nov. 28, 2000).

packages for the selected systems to assess the extent to which the components implemented key information security practices and controls. Certification is a comprehensive process of assessing the level of security risk, identifying security controls needed to reduce risk and maintain it at an acceptable level, documenting security controls in a security plan, and testing controls to ensure they operate as intended. Accreditation is a written decision by an agency management official authorizing operation of a particular information system or group of systems. Specifically, we reviewed and analyzed information security plans, risk assessments, information security test and evaluation reports, remedial action plans, and continuity of operations plans for the selected systems. We compared the components' documented practices and controls for these information security areas with applicable FISMA requirements, OMB guidance, and applicable NIST guidance.

To supplement our documentation reviews and analysis, we reviewed and considered various audit reports from the CIO and OIG evaluations of DHS's information security program, including DHS's and OIG's annual FISMA reports from 2003 and 2004.

We performed our review at DHS headquarters, the offices of the seven components, and at our headquarters in the Washington, D.C., metropolitan area; and at DHS's network and security operations center in Denver, Colorado, from July 2004 through May 2005. Our review was performed in accordance with generally accepted government auditing standards.

Comments from the Department of Homeland Security



Washington, DC 20528

Homeland Security

June 13, 2005

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

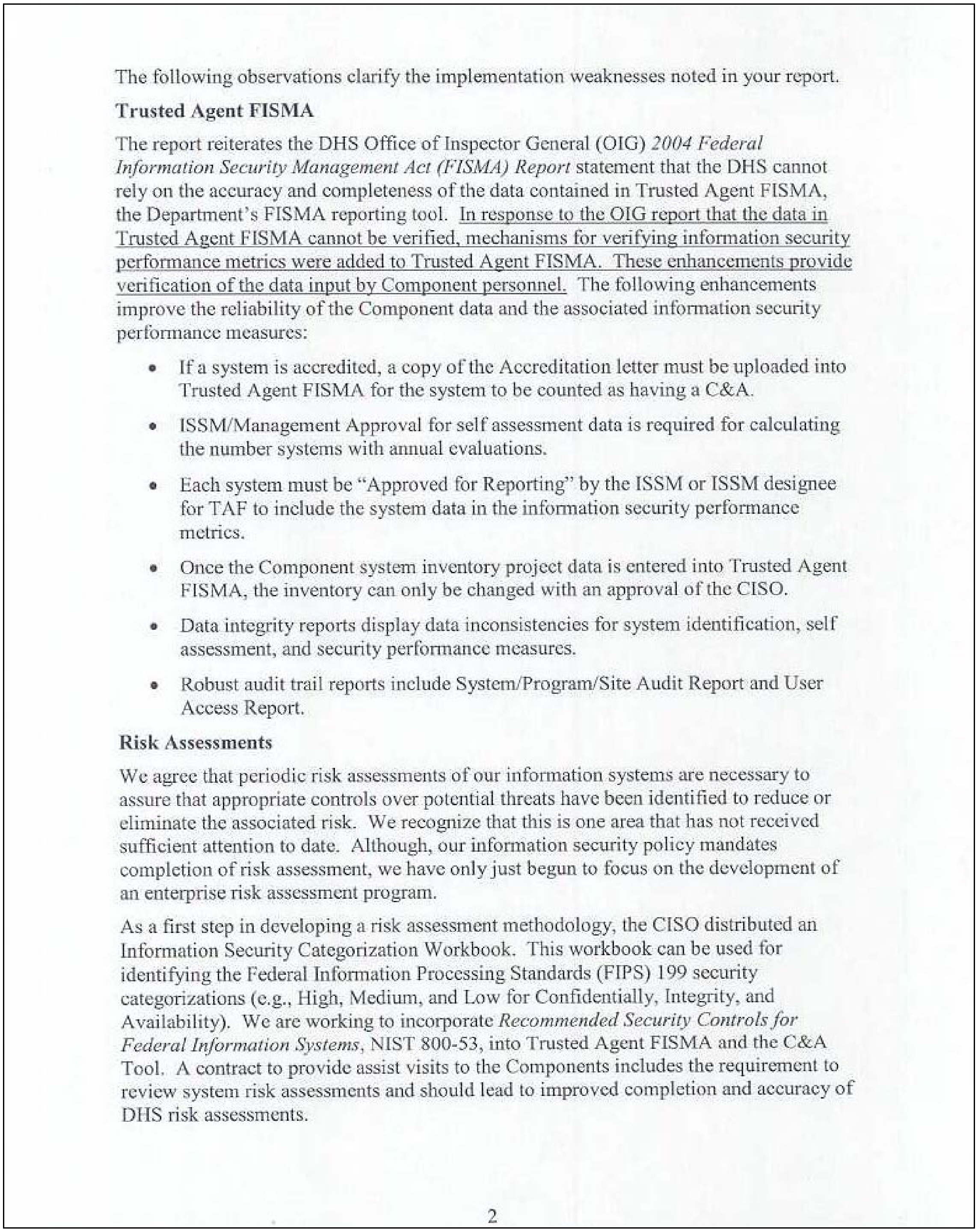
Subject: Response to June 2005 GAO Information Security Report (GAO-05-700)

Thank you for the opportunity to provide comments on your draft review of the Department of Homeland Security (DHS) Information Security Program. We appreciate that the draft report acknowledges the progress that DHS has made in implementing its Information Security Program and the management challenges that the Department faces as it continues to merge the information security programs of the 22 legacy agencies.

As noted in your report, "the Chief Information Security Officer (CISO) has made significant progress in developing and documenting a department-wide information security program." We continually strive to improve and enhance the program based on suggestions from our stakeholders, the lessons learned in the past two years, and emerging needs of our customers. Our efforts are aimed at supporting the program's mission to ensure that DHS has a secure and trusted computing environment based on sound risk management principles that enables the Department to effectively share information in support of its mission.

However, we have accomplished more than document a department-wide information security program. We are, in fact, investing significant resources in program implementation. Central to that is an ongoing effort to complete a Department-wide systems and applications inventory. We are scheduled to be completed in early August of this year, and we will then have a comprehensive and consistent baseline for program management and compliance in the future. We have also completed a success pilot of the DHS enterprise Certification and Accreditation (C&A) Tool, and that tool was fully functional as an enterprise application on April 11th. The tool provides the capabilities to resolve issues with the Security Plans, Testing and Evaluation, and Continuity of Operations. The tool automates many critical C&A activities and will standardize the content and format of security accreditation packages. Department policy mandates the use of the C&A Tool for all new accreditation packages.

From April 11th through June 1, 335 new accreditation packages were initiated in the DHS C&A Tool. The CISO is funding numerous training classes to familiarize users with the tool features. In addition, the tool vendor is providing one-on-one assistance to the Component Information Security System Managers (ISSMs) and their staff to resolve implementation issues and to customize the tool to incorporate Component specific baseline security requirements.



The following observations clarify the implementation weaknesses noted in your report.

Trusted Agent FISMA

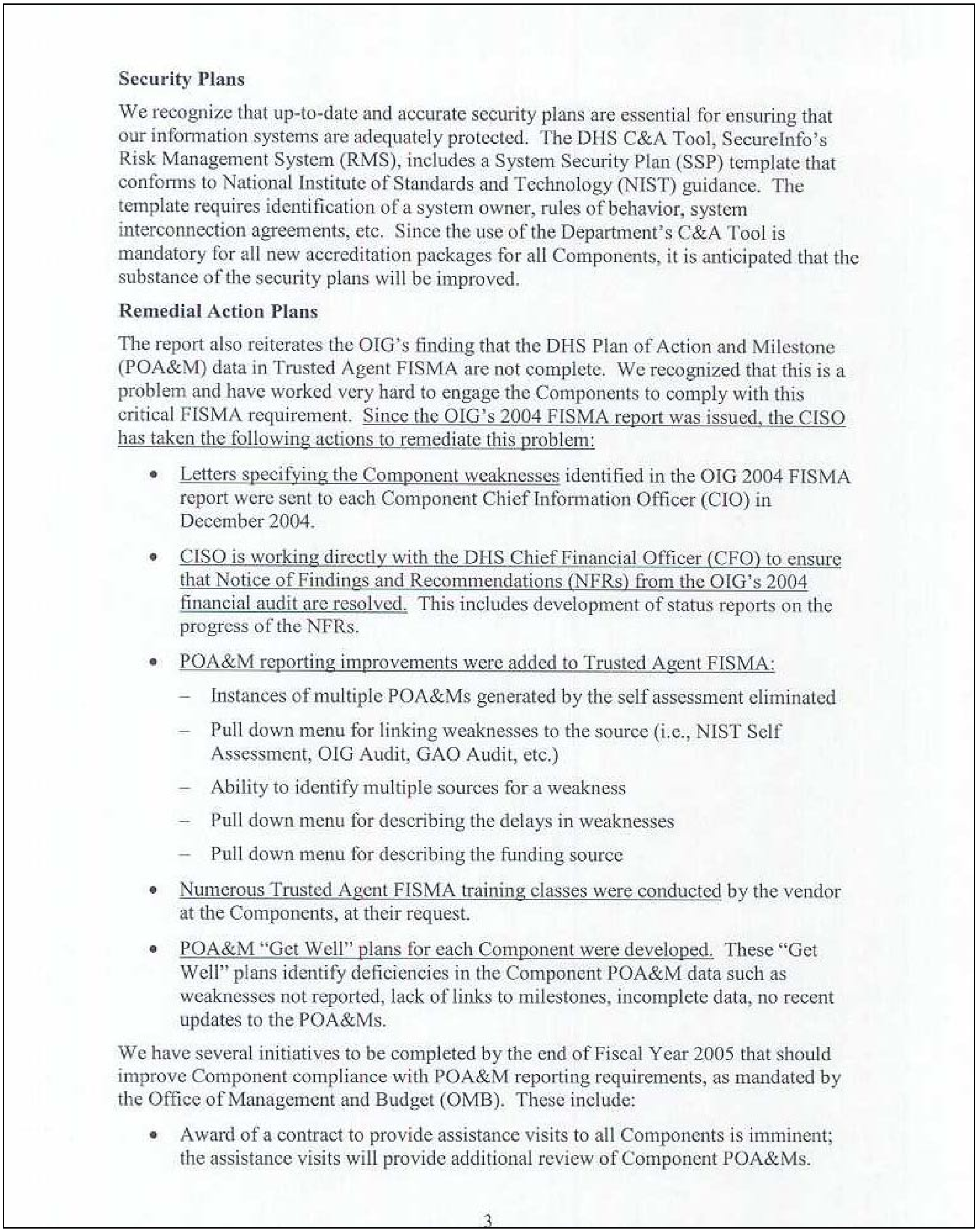
The report reiterates the DHS Office of Inspector General (OIG) *2004 Federal Information Security Management Act (FISMA) Report* statement that the DHS cannot rely on the accuracy and completeness of the data contained in Trusted Agent FISMA, the Department's FISMA reporting tool. In response to the OIG report that the data in Trusted Agent FISMA cannot be verified, mechanisms for verifying information security performance metrics were added to Trusted Agent FISMA. These enhancements provide verification of the data input by Component personnel. The following enhancements improve the reliability of the Component data and the associated information security performance measures:

- If a system is accredited, a copy of the Accreditation letter must be uploaded into Trusted Agent FISMA for the system to be counted as having a C&A.
- ISSM/Management Approval for self assessment data is required for calculating the number systems with annual evaluations.
- Each system must be "Approved for Reporting" by the ISSM or ISSM designee for TAF to include the system data in the information security performance metrics.
- Once the Component system inventory project data is entered into Trusted Agent FISMA, the inventory can only be changed with an approval of the CISO.
- Data integrity reports display data inconsistencies for system identification, self assessment, and security performance measures.
- Robust audit trail reports include System/Program/Site Audit Report and User Access Report.

Risk Assessments

We agree that periodic risk assessments of our information systems are necessary to assure that appropriate controls over potential threats have been identified to reduce or eliminate the associated risk. We recognize that this is one area that has not received sufficient attention to date. Although, our information security policy mandates completion of risk assessment, we have only just begun to focus on the development of an enterprise risk assessment program.

As a first step in developing a risk assessment methodology, the CISO distributed an Information Security Categorization Workbook. This workbook can be used for identifying the Federal Information Processing Standards (FIPS) 199 security categorizations (e.g., High, Medium, and Low for Confidentially, Integrity, and Availability). We are working to incorporate *Recommended Security Controls for Federal Information Systems*, NIST 800-53, into Trusted Agent FISMA and the C&A Tool. A contract to provide assist visits to the Components includes the requirement to review system risk assessments and should lead to improved completion and accuracy of DHS risk assessments.



Security Plans

We recognize that up-to-date and accurate security plans are essential for ensuring that our information systems are adequately protected. The DHS C&A Tool, SecureInfo's Risk Management System (RMS), includes a System Security Plan (SSP) template that conforms to National Institute of Standards and Technology (NIST) guidance. The template requires identification of a system owner, rules of behavior, system interconnection agreements, etc. Since the use of the Department's C&A Tool is mandatory for all new accreditation packages for all Components, it is anticipated that the substance of the security plans will be improved.

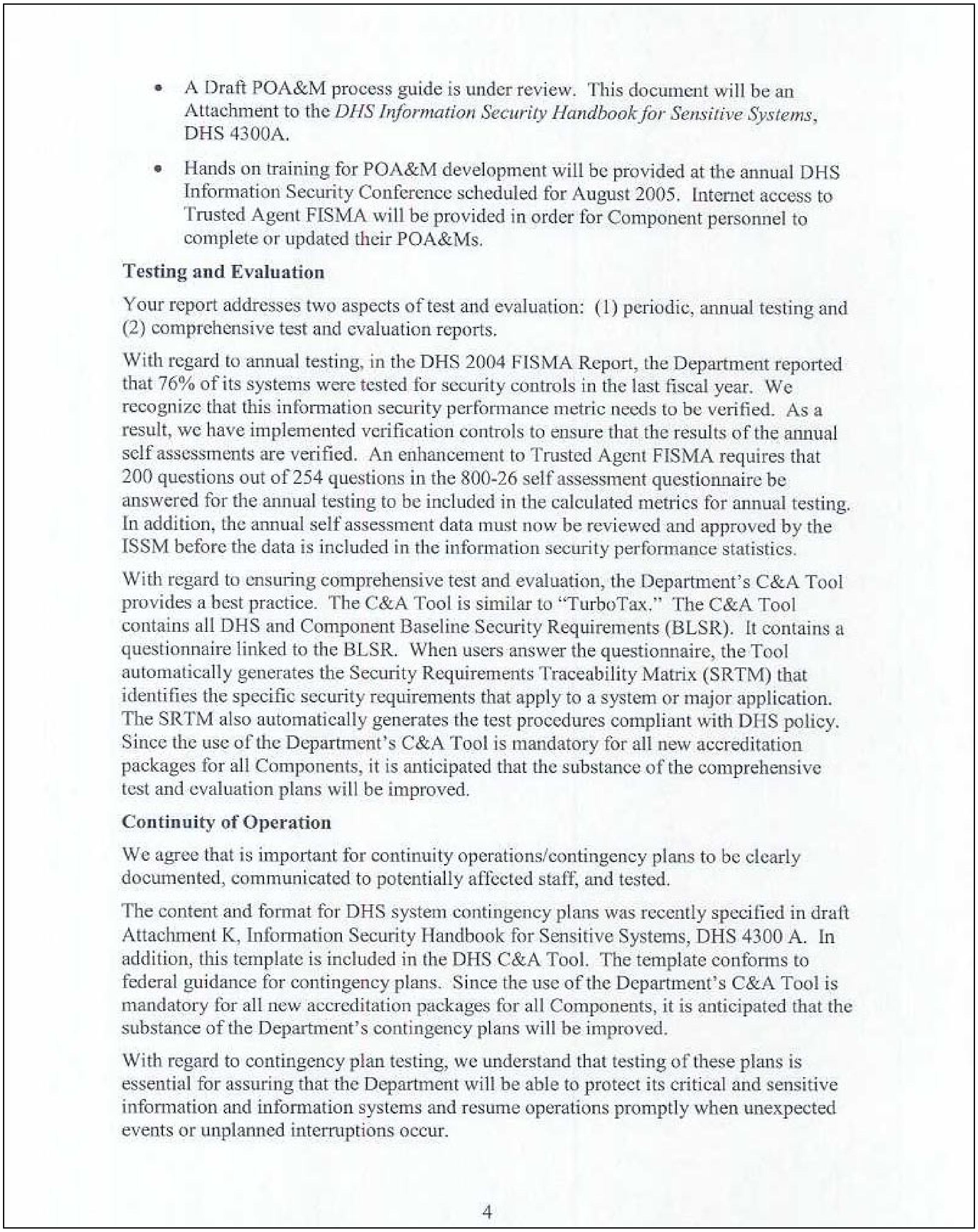
Remedial Action Plans

The report also reiterates the OIG's finding that the DHS Plan of Action and Milestone (POA&M) data in Trusted Agent FISMA are not complete. We recognized that this is a problem and have worked very hard to engage the Components to comply with this critical FISMA requirement. Since the OIG's 2004 FISMA report was issued, the CISO has taken the following actions to remediate this problem:

- Letters specifying the Component weaknesses identified in the OIG 2004 FISMA report were sent to each Component Chief Information Officer (CIO) in December 2004.
- CISO is working directly with the DHS Chief Financial Officer (CFO) to ensure that Notice of Findings and Recommendations (NFRs) from the OIG's 2004 financial audit are resolved. This includes development of status reports on the progress of the NFRs.
- POA&M reporting improvements were added to Trusted Agent FISMA:
  - Instances of multiple POA&Ms generated by the self assessment eliminated
  - Pull down menu for linking weaknesses to the source (i.e., NIST Self Assessment, OIG Audit, GAO Audit, etc.)
  - Ability to identify multiple sources for a weakness
  - Pull down menu for describing the delays in weaknesses
  - Pull down menu for describing the funding source
- Numerous Trusted Agent FISMA training classes were conducted by the vendor at the Components, at their request.
- POA&M "Get Well" plans for each Component were developed. These "Get Well" plans identify deficiencies in the Component POA&M data such as weaknesses not reported, lack of links to milestones, incomplete data, no recent updates to the POA&Ms.

We have several initiatives to be completed by the end of Fiscal Year 2005 that should improve Component compliance with POA&M reporting requirements, as mandated by the Office of Management and Budget (OMB). These include:

- Award of a contract to provide assistance visits to all Components is imminent; the assistance visits will provide additional review of Component POA&Ms.



- A Draft POA&M process guide is under review. This document will be an Attachment to the *DHS Information Security Handbook for Sensitive Systems*, DHS 4300A.
- Hands on training for POA&M development will be provided at the annual DHS Information Security Conference scheduled for August 2005. Internet access to Trusted Agent FISMA will be provided in order for Component personnel to complete or updated their POA&Ms.

Testing and Evaluation

Your report addresses two aspects of test and evaluation: (1) periodic, annual testing and (2) comprehensive test and evaluation reports.

With regard to annual testing, in the DHS 2004 FISMA Report, the Department reported that 76% of its systems were tested for security controls in the last fiscal year. We recognize that this information security performance metric needs to be verified. As a result, we have implemented verification controls to ensure that the results of the annual self assessments are verified. An enhancement to Trusted Agent FISMA requires that 200 questions out of 254 questions in the 800-26 self assessment questionnaire be answered for the annual testing to be included in the calculated metrics for annual testing. In addition, the annual self assessment data must now be reviewed and approved by the ISSM before the data is included in the information security performance statistics.

With regard to ensuring comprehensive test and evaluation, the Department's C&A Tool provides a best practice. The C&A Tool is similar to "TurboTax." The C&A Tool contains all DHS and Component Baseline Security Requirements (BLSR). It contains a questionnaire linked to the BLSR. When users answer the questionnaire, the Tool automatically generates the Security Requirements Traceability Matrix (SRTM) that identifies the specific security requirements that apply to a system or major application. The SRTM also automatically generates the test procedures compliant with DHS policy. Since the use of the Department's C&A Tool is mandatory for all new accreditation packages for all Components, it is anticipated that the substance of the comprehensive test and evaluation plans will be improved.

Continuity of Operation

We agree that is important for continuity operations/contingency plans to be clearly documented, communicated to potentially affected staff, and tested.

The content and format for DHS system contingency plans was recently specified in draft Attachment K, Information Security Handbook for Sensitive Systems, DHS 4300 A. In addition, this template is included in the DHS C&A Tool. The template conforms to federal guidance for contingency plans. Since the use of the Department's C&A Tool is mandatory for all new accreditation packages for all Components, it is anticipated that the substance of the Department's contingency plans will be improved.

With regard to contingency plan testing, we understand that testing of these plans is essential for assuring that the Department will be able to protect its critical and sensitive information and information systems and resume operations promptly when unexpected events or unplanned interruptions occur.

In order to ensure that all Components identify critical and sensitive information DHS, in March 2005, the CISO began distributing an Information Security Categorization Workbook. This workbook can be used for identifying the FIPS 199 security categorizations (e.g., High, Medium, and Low for Confidentially, Integrity, and Availability).

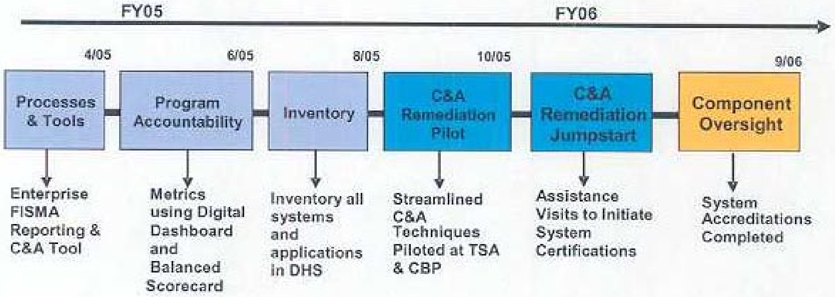
Identification of critical and sensitive DHS information is an important first step in solving the contingency plan issues.

Conclusion and Path Forward

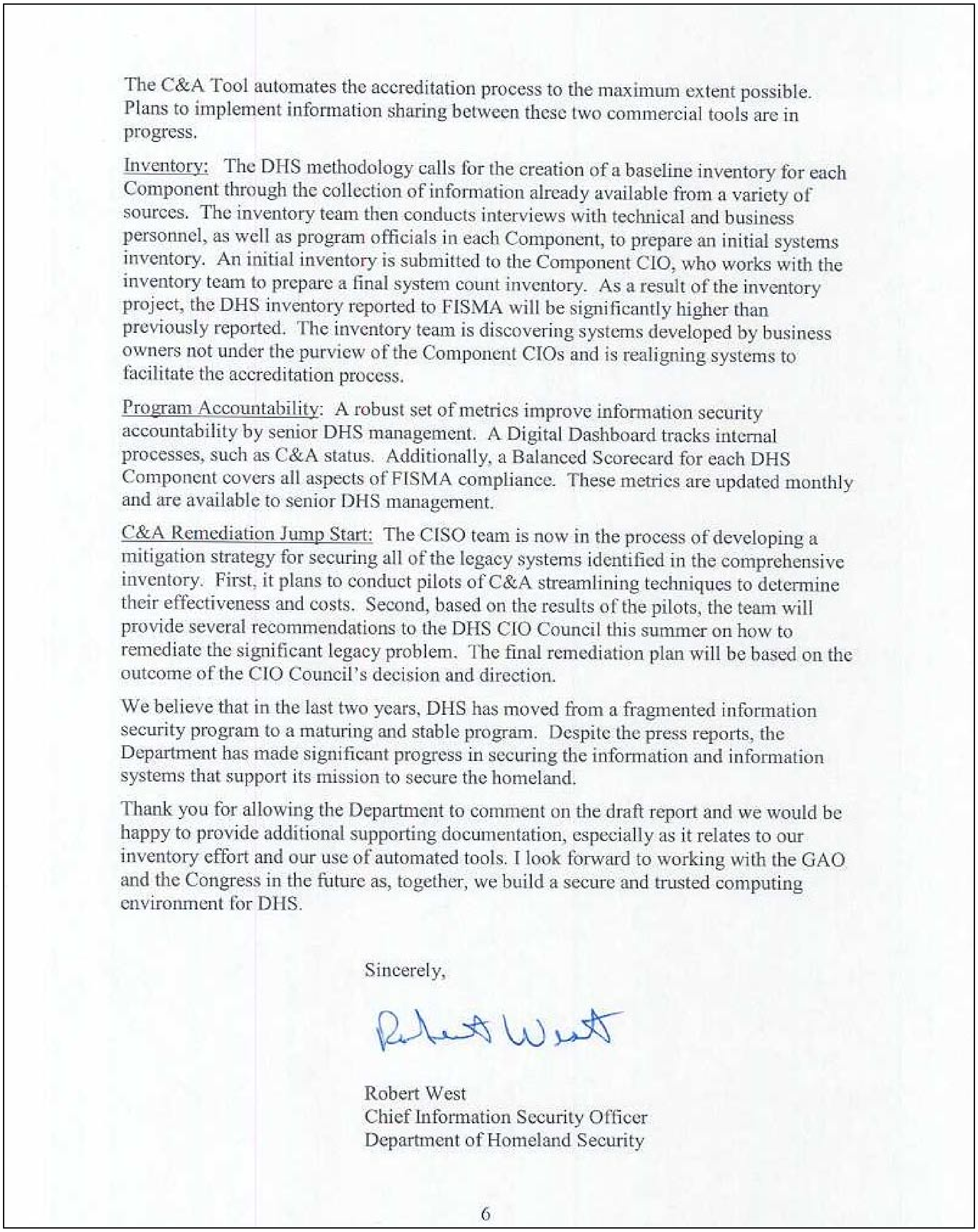
In conclusion, negative reviews of the DHS Information Security Program are a result of the following pervasive institutional impediments:

- Inaccurate legacy organization inventories
- IT systems fielded by mission owners outside the purview of the CIO
- Inadequate certification and accreditation (C&A) of information systems
- Institutional resistance to new processes and procedures
- General lack of accountability for information security

The strategy the DHS CISO team is implementing to overcome these impediments to program implementation is illustrated below. This strategy builds on the successful initiatives that were implemented in Fiscal Year 2004.


FY05
FY06
4/05
6/05
8/05
10/05
9/06
Processes & Tools
Program Accountability
Inventory
C&A Remediation Pilot
C&A Remediation Jumpstart
Component Oversight
Enterprise FISMA Reporting & C&A Tool
Metrics using Digital Dashboard and Balanced Scorecard
Inventory all systems and applications in DHS
Streamlined C&A Techniques Piloted at TSA & CBP
Assistance Visits to Initiate System Certifications
System Accreditations Completed

Processes and Tools: Two enterprise, web-based, security management tools are operational and are intended to reduce the cost of security management activities. A FISMA reporting tool, Trusted Agent FISMA, automates the POA&M process, annual test and evaluation, inventory management, and FISMA report development.



The C&A Tool automates the accreditation process to the maximum extent possible. Plans to implement information sharing between these two commercial tools are in progress.

Inventory: The DHS methodology calls for the creation of a baseline inventory for each Component through the collection of information already available from a variety of sources. The inventory team then conducts interviews with technical and business personnel, as well as program officials in each Component, to prepare an initial systems inventory. An initial inventory is submitted to the Component CIO, who works with the inventory team to prepare a final system count inventory. As a result of the inventory project, the DHS inventory reported to FISMA will be significantly higher than previously reported. The inventory team is discovering systems developed by business owners not under the purview of the Component CIOs and is realigning systems to facilitate the accreditation process.

Program Accountability: A robust set of metrics improve information security accountability by senior DHS management. A Digital Dashboard tracks internal processes, such as C&A status. Additionally, a Balanced Scorecard for each DHS Component covers all aspects of FISMA compliance. These metrics are updated monthly and are available to senior DHS management.

C&A Remediation Jump Start: The CISO team is now in the process of developing a mitigation strategy for securing all of the legacy systems identified in the comprehensive inventory. First, it plans to conduct pilots of C&A streamlining techniques to determine their effectiveness and costs. Second, based on the results of the pilots, the team will provide several recommendations to the DHS CIO Council this summer on how to remediate the significant legacy problem. The final remediation plan will be based on the outcome of the CIO Council's decision and direction.

We believe that in the last two years, DHS has moved from a fragmented information security program to a maturing and stable program. Despite the press reports, the Department has made significant progress in securing the information and information systems that support its mission to secure the homeland.

Thank you for allowing the Department to comment on the draft report and we would be happy to provide additional supporting documentation, especially as it relates to our inventory effort and our use of automated tools. I look forward to working with the GAO and the Congress in the future as, together, we build a secure and trusted computing environment for DHS.

Sincerely,

Robert West

Robert West
Chief Information Security Officer
Department of Homeland Security

6

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; Joanne Fiorino; Kenneth A. Johnson; Lori Martinez; Leena Mathew; and Altony Rice 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