United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

For Release on Delivery
2:00 p.m. EDT
Wednesday, June 20, 2007

INFORMATION SECURITY

Homeland Security Needs to Enhance Effectiveness of Its Program

Statement of

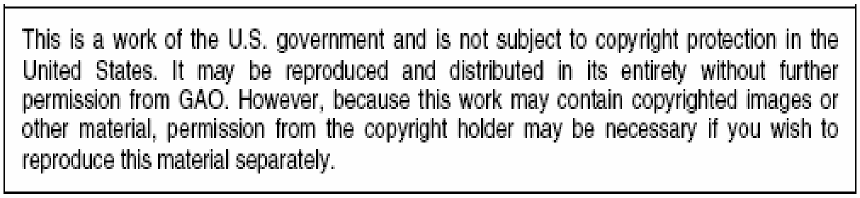
Gregory C. Wilshusen
Director, Information Security Issues

Keith A. Rhodes,
Chief Technologist

Accountability * Integrity * Reliability

Abbreviations

CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
IG	inspector general



G A O
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-1003T, a testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

To protect and mitigate threats and attacks against the United States, 22 federal agencies and organizations were merged to form the Department of Homeland Security (DHS) in 2002. One of the department's components, U.S. Customs and Border Protection (CBP), is responsible for securing the nation's borders. DHS and CBP rely on a variety of computerized information systems to support their operations and assets.

GAO has reported for many years that poor information security is a widespread problem with potentially devastating consequences. In reports to Congress since 1997, GAO has identified information security as a governmentwide high-risk issue.

In this testimony, GAO discusses DHS's information security program and computer security controls for key information systems. GAO based its testimony on agency, inspector general, and GAO issued and draft reports on DHS information security.

What GAO Recommends

To enhance departmental security, GAO has previously made recommendations to DHS in implementing its information security program and is making additional recommendations in two draft reports currently being reviewed by the department.

www.gao.gov/cgi-bin/getrpt?GAO-07-1003T

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen, wilshuseng@gao.gov, (202) 512-6244, or Keith A. Rhodes, rhodesk@gao.gov, (202) 512-6412.

June 20, 2007

INFORMATION SECURITY

Homeland Security Needs to Enhance Effectiveness of Its Program

What GAO Found

Shortcomings in DHS's information security program remain, although progress has been made. In 2005, GAO reported that DHS had not fully implemented a comprehensive, departmentwide information security program to protect the information and information systems that support its operations and assets. For example, the department did not have a complete inventory of its systems, and component agencies did not fully or effectively perform key program activities such as developing risk assessments, preparing security plans, testing and evaluating the effectiveness of security controls, completing remedial action plans, and developing and testing continuity of operations plans. GAO recommended that DHS take specific actions to address these problems. Since then, DHS has taken steps to improve its security program. In fiscal year 2006, it prepared a complete inventory of its major applications and systems for the first time. DHS has also implemented key program activities—such as contingency plan testing, security control testing, and system certification and accreditation—on an increasing percentage of its systems. However, the quality or effectiveness of these activities was not assured and deficiencies continue to exist.

These program deficiencies contribute to significant weaknesses in computer security controls that threaten the confidentiality, integrity, and availability of key DHS information and information systems. For example, DHS's independent auditors reported that security over the department's financial systems was a material weakness in internal control for fiscal year 2006. In addition, GAO determined that CBP did not implement controls to effectively prevent, limit, and detect access to certain computer networks, systems, and information since it did not (1) adequately identify and authenticate users; (2) sufficiently limit access to information and information systems; (3) ensure that controls adequately protected external and internal boundaries; (4) effectively implement physical security at several locations; (5) consistently encrypt sensitive data traversing the communication network; and (6) provide adequate logging or user accountability for the mainframe, workstations, or servers. CBP also did not always ensure that responsibilities for system development and system production were sufficiently segregated. As a result, increased risk exists that unauthorized individuals, internal and external to the organization, could read, copy, delete, add, and modify sensitive and personally identifiable information and disrupt service on DHS systems.

Until DHS and its components act to fully and effectively implement the department's security program and mitigate known weaknesses, they will have limited assurance that sensitive information and computer systems will be sufficiently safeguarded or that departmental missions and goals will be achieved. Implementation of GAO's recommendations will assist DHS in mitigating the deficiencies described above.

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to participate in today's hearing on information security at the Department of Homeland Security (DHS). Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies such as DHS, where the public's trust is essential. For many years, GAO has reported that poor information security is a widespread problem with potentially devastating consequences. In reports to the Congress since 1997,[1] GAO identified information security as a governmentwide high-risk issue.

In this testimony, we discuss DHS's departmentwide information security program and computer security controls for key information systems. We based this testimony, in part, on our previously issued reports[2] and our draft report—which has been provided to DHS for review and comment—on computer security controls for certain information systems operated by U.S. Customs and Border Protection (CBP). We also considered our analysis of the department's annual Federal Information Security Management Act (FISMA)[3] reports for 2005 and 2006 and the department's performance and accountability report for 2006. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

[1] GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

[2] GAO, Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program, GAO-05-700 (Washington, D.C.: June 2005) and Information Security: Department of Homeland Security Faces Challenges in Fulfilling Statutory Requirements, GAO-05-567T (Washington, D.C.: April 2005).

[3] FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002) and requires agencies and their inspectors general or independent external auditors to report annually on the effectiveness of their security policies and compliance with the requirements of the Act. GAO, *Information Security: Agencies Report Progress But Sensitive Data Remains at Risk*, GAO-07-935T (Washington, D.C.: June 2007) describes the results of GAO's analysis of the 2006 FISMA reports for 24 agencies including DHS.

Results in Brief

Shortcomings in DHS's information security program remain, although progress has been made. In 2005, we reported that DHS had not fully implemented a comprehensive, departmentwide information security program to protect the information and information systems that support its operations and assets. For example, the department did not have a complete inventory of its systems and component agencies did not fully or effectively perform key program activities such as developing risk assessments, preparing security plans, testing and evaluating the effectiveness of security controls, completing remedial action plans, and developing and testing continuity of operations plans. We recommended that DHS take specific actions to address these problems. Since our 2005 report, DHS has taken steps to improve its security program. In fiscal year 2006, DHS completed its first comprehensive inventory of its major applications and systems. DHS has also implemented a departmentwide tool that incorporates the guidance required to adequately complete a certification and accreditation for all systems and has implemented key program activities—such as contingency plan testing, security control testing, and system certification and accreditation—on an increasing percentage of its systems. However, the quality or effectiveness of these activities was not assured and deficiencies continue to exist.

These program deficiencies contribute to significant weaknesses in computer security controls that threaten the confidentiality, integrity, and availability of key DHS information and information systems. For example, DHS's independent auditors reported that security over the department's financial systems was a material weakness in internal control for fiscal year 2006. In addition, GAO determined that CBP did not implement controls to effectively prevent, limit, and detect access to certain computer networks, systems, and information since it did not (1) adequately identify and authenticate users; (2) sufficiently limit access to information and information systems; (3) ensure that controls adequately protected external and internal boundaries; (4) effectively implement physical security at several locations; (5) consistently encrypt sensitive data traversing the communication network; and (6) provide adequate logging or user accountability for the mainframe, workstations, or servers. CBP also did not always ensure that responsibilities for system development and system production were sufficiently segregated. As a result, increased risk exists that unauthorized individuals, internal and external to the organization, could read, copy, delete, add, and modify sensitive and personally identifiable information and disrupt service on DHS systems.

Until DHS and its components act to fully and effectively implement its security program and mitigate known weaknesses, they will have limited assurance that sensitive information and computer systems will be sufficiently safeguarded or that departmental missions and goals will be achieved. Implementation of GAO's recommendations will assist DHS in mitigating the deficiencies described in this statement.

Background

To address the challenge of responding to current and potential threats to homeland security—one of the federal government's most significant challenges—the Homeland Security Act of 2002 mandated the merging of 22 federal agencies and organizations to create DHS. Not since the creation of the Department of Defense in 1947 has the federal government undertaken a transformation of this magnitude. Each of the 22 agencies and organizations brought their own management challenges, distinct missions, unique information technology infrastructures and systems, and policies and procedures, thereby making the implementation and integration of an effective departmentwide information security program a significant challenge.

DHS's mission, in part, is to prevent and deter terrorist attacks within the United States,[4] reduce the vulnerability of the United States to terrorism, and to minimize the damage and assist in the

[4] 6 U.S.C. § 113(a).

recovery from terrorist attacks that do occur.[5] One of the department's components, CBP, is responsible for securing the nation's borders.

Virtually all DHS and CBP operations are supported by automated systems and electronic data, and the agency would find it difficult, if not impossible, to carry out its mission and account for its resources without these information assets. Hence, the degree of risk caused by security weaknesses is high. For example, as a result of such weaknesses, resources (such as payments and collections) could be lost or stolen, data could be modified or destroyed, and computer resources could be used for unauthorized purposes or to launch attacks on other computer systems. Sensitive information could be inappropriately disclosed, browsed, or copied for improper or criminal purposes. Critical operations could be disrupted, such as those supporting homeland security and emergency services. Finally, DHS's missions could be undermined by embarrassing incidents, diminishing confidence in its ability to conduct operations and fulfill its fiduciary responsibilities.

According to FISMA, the Secretary of DHS is responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems used by the agency or by a contractor on behalf of the agency. The Secretary has delegated to the DHS Chief Information Officer (CIO) responsibility for ensuring compliance with federal information security requirements and reporting annually to the Secretary on the effectiveness of the department's information security program. The CIO designated the Chief Information Security Officer (CISO) to

- develop and maintain a departmentwide information security program, as required by FISMA;

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

[5] 6 U.S.C. § 111(b).

- provide the direction and guidance necessary to ensure that information security throughout the department is compliant with federal and departmental information security requirements and policies; and
- advise the CIO on the status and issues involving security aspects of the departmentwide information security program.

Shortcomings in DHS Information Security Program Remain Although Progress Has Been Made

In 2005, GAO reported[6] that DHS had not fully or effectively implemented a comprehensive, departmentwide information security program to protect the information and information systems that support its operations and assets. Although DHS had developed and documented policies and procedures that could provide a framework for implementing the department's program, certain departmental components had not yet fully implemented key program activities. Components' weaknesses in implementing these activities included (1) incomplete risk assessments for determining the required controls and the level of resources that should be expended on them; (2) missing required elements from information system security plans for providing a full understanding of the existing and planned information security requirements; (3) incomplete or nonexistent test and evaluation of security controls for determining the effectiveness of information security policies and procedures; (4) missing required elements from remedial action plans for identifying the resources needed to correct or mitigate identified information security weaknesses; and (5) incomplete, nonexistent, or untested continuity of operations plans for restoring critical systems in the case of unexpected events.

The table below indicates with an "x" where GAO found weaknesses with key information security program activities for six systems and applications reviewed at four components.

[6] GAO-05-700.

Table 1: Weaknesses in Information Security Program Activities for Selected Systems

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 Visitor 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.

We also reported that DHS had not yet fully developed a complete and accurate systems inventory and had used an enterprise management tool (known as Trusted Agent FISMA) that contained unreliable data for overseeing the components' reported performance data on their compliance with key information security activities. The DHS Inspector General reported that the data in the tool were not verified, there was no audit trail capability, material weaknesses were not consistently reported or linked to plans of action and milestones, and plans of action and milestones that had been identified and documented were not current.

To assist DHS in addressing these issues, we recommended that it establish milestones for verifying the components' reported performance data in Trusted Agent FISMA and instruct its component agencies to

- develop complete risk assessments;
- document comprehensive security plans;
- fully perform testing and evaluation of security controls;

- complete remedial action plans; and
- develop, document, and test continuity of operations plans.

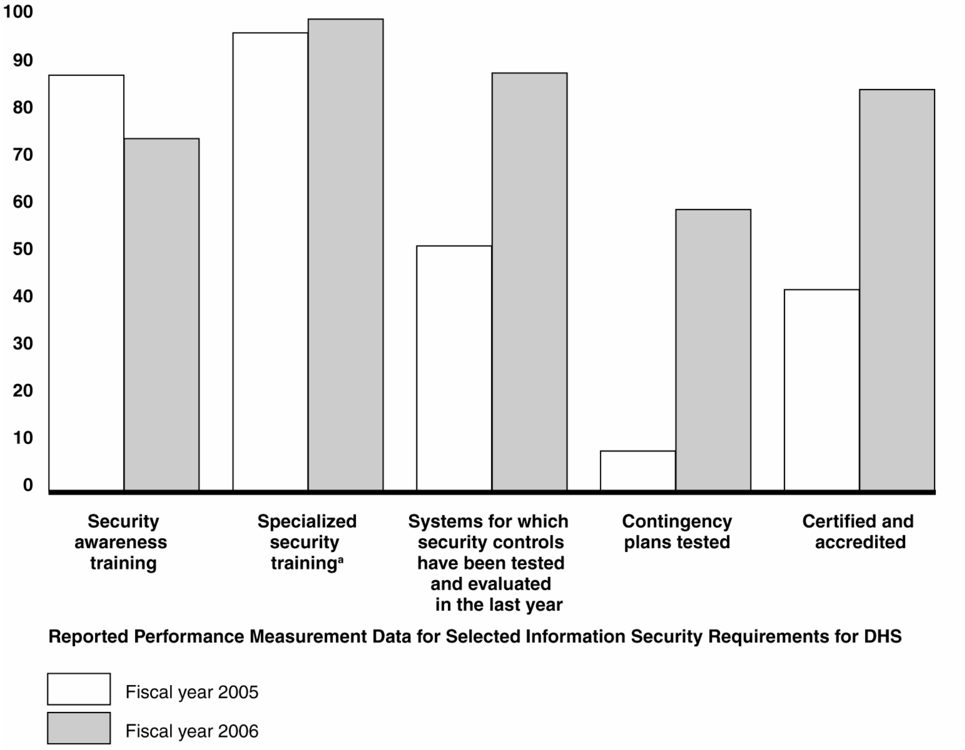
DHS Has Taken Steps to Improve Security Program, but Deficiencies Persist

In response to our recommendations, the department has made several improvements in its information security program. For example, DHS officials stated that they had developed a plan to address all of the recommendations in our 2005 report. For the first time since its creation, DHS completed a comprehensive inventory of its major applications and general support systems, including contractor and national security systems, for all organizational components in fiscal year 2006. DHS also implemented a departmentwide tool that incorporated the guidance required to complete a certification and accreditation[7] for all systems. The completion of these two tasks eliminated two factors that had significantly impeded the department from achieving some success in establishing its security program over the previous two years. In addition, the CISO revised the baseline information technology security policies and procedures and mandated that the components ensure that their systems meet the requirements specified in the DHS baseline configuration guides.

With the exception of providing security awareness training to employees, the department has also implemented key program activities such as conducting specialized security training, testing and evaluating controls, testing contingency plans, and certifying and accrediting systems, for an increasing percentage of its systems or personnel in fiscal year 2006 (see figure below).

[7] Certification is the comprehensive evaluation of the management, operational, and technical security controls in an information system to determine the effectiveness of these controls and identify existing vulnerabilities. Accreditation is the official management decision to authorize operation of an information system. This authorization explicitly accepts the risk remaining after the implementation of an agreed-upon set of security controls.

Performance Measure Percentages for Selected Information Security Requirements



Source: GAO analysis of DHS FISMA reports.

However, the quality or effectiveness of certain information security program activities has not been assured. Although CBP has made important progress in implementing the department's information security program, it has not fully or effectively implemented key program activities. For example,

- risk assessments performed for systems supporting a key border protection program did not always fully characterize risks to the systems;
- interconnection security agreements listed in the security plan for a key system were not current;
- procedures for testing and evaluating the effectiveness of security controls were not sufficient and did not reveal problems with a mainframe computer that potentially allowed unauthorized users to read, copy, change, delete, and modify sensitive information;

- CBP did not always address significant deficiencies in a remedial action plan thereby exposing sensitive information to increased risk of unauthorized disclosure or modification;
- CBP did not adequately establish and implement tools and processes to ensure timely detection and handling of security incidents; and
- CBP had incomplete or out-of-date privacy documents for systems supporting a key border protection program.

Significant Control Weaknesses Place Sensitive Information and Operations at Risk

Significant weaknesses in computer security controls threaten the confidentiality, integrity, and availability of key DHS information and information systems.

Independent external auditors identified over 130 information technology control weaknesses affecting the department's financial systems during the audit of its fiscal year 2006 financial statements. Weaknesses existed in all key general controls and application controls. For example,

- systems were not certified and accredited in accordance with departmental policy;
- policies and procedures for incident response were inadequate;
- background investigations were not properly conducted; and
- security awareness training did not always comply with departmental requirements.

Additionally, users had weak passwords on key servers that process and house DHS financial data, and workstations, servers, and network devices were configured without necessary security patches. Further, changes to sensitive operating system settings were not always documented; individuals were able to perform incompatible duties such as changing, testing, and implementing software; and service continuity plans were not consistently or adequately tested. As a result, material errors in DHS's financial data may not be detected in a timely manner.

Although CBP has made progress in addressing security vulnerabilities, significant problem areas still remain. Certain CBP systems supporting a key border protection program were riddled with control weaknesses that placed sensitive and personally identifiable information at increased risk of unauthorized disclosure and modification, misuse, and destruction possibly without detection, and placed program operations at increased risk of disruption. Weaknesses existed in all control areas and computing device types reviewed. Deficiencies in controls intended to prevent, limit, and detect access to information and information systems exposed CBP's mainframe computer, network infrastructure, servers, and workstations to insider and external threats, as the following examples demonstrate. Specifically, CBP did not

- adequately identify and authenticate users in systems; for example, passwords were transmitted over the network in clear text and were stored using weak encryption;

- sufficiently limit access to information and information systems; for example, over one thousand users with command line access could put a program designed to bypass security rules into a special system library;

- ensure that controls adequately protected external and internal network boundaries; for example, internal network traffic was not segregated; moreover, workstations and many servers did not have host based firewalls;

- effectively implement physical security at several locations; for example, CBP did not control access to its restricted information technology spaces since its physical access systems were controlled by local authorities;

- consistently apply encryption to protect sensitive data traversing the communication network; for example, network routers, switches, and network management servers used unencrypted network protocols so that files traversing the network could be read;

- adequately provide audit logging or user accountability for the mainframe computer, workstations, or servers; for example, monitoring lists for key operating system libraries did not capture needed data for all sensitive libraries in the desired locations;

- always ensure that responsibilities for system development and system operations or production were sufficiently segregated; for example, mainframe system programmers were allowed to access application production data and developmental staff could access mainframe operating system libraries; moreover, developmental staff had update access to the application production data;

- consistently maintain secure configurations on the mainframe, applications servers, and workstations we reviewed at the data center and ports of entry; for example, production servers and workstations were missing critical operating system and software application security patches.

As a result, increased risk exists that unauthorized individuals, internal and external to the organization could read, delete, add, and modify sensitive and personally identifiable information and disrupt service on DHS systems.

To assist enhance departmental security, GAO has previously made recommendations to DHS in implementing its information security program and is making additional recommendations in two draft reports currently being reviewed by the department. Implementation of these recommendations will facilitate improvements in the department's information security posture.

In summary, DHS has made progress in implementing its departmentwide information security program. However, the effectiveness of its program is not assured. Deficiencies in key program activities continue to exist and contribute to significant computer security control weaknesses that place (1) sensitive information and information systems at increased risk of unauthorized disclosure, use, modification, or destruction, possibly without detection, and (2) agency operations at risk of disruption.

Ensuring that weaknesses are promptly mitigated and that controls are effective will require senior management support and leadership, disciplined processes, and effective coordination between DHS and its components. It also requires consistent oversight from the Secretary of DHS and the Congress. Until DHS and its components act to fully and effectively implement the department's information security program and mitigate known weaknesses, limited assurance will exist that sensitive information will be sufficiently safeguarded against unauthorized disclosure, modification, and destruction, or that DHS components will achieve their goals.

Mr. Chairman, this concludes our statement. We would be happy to answer your questions.

Contacts and Acknowledgements

If you have any questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or Keith A. Rhodes at (202) 512-6412. We can also be reached by e-mail at wilshuseng@gao.gov or rhodesk@gao.gov, respectively.

Other key contributors to this statement include Bill Wadsworth (Assistant Director), Ed Alexander, Lon Chin, West Coile, Kirk Daubenspeck, Neil Doherty, Patrick Dugan, Denise Fitzpatrick, Ed Glagola, David Hayes, David Plocher, Henry Sutanto, Amos Tevelow, and Christopher Warweg.

(310599)