June 20, 2007

INFORMATION SECURITY

Homeland Security Needs to Enhance Effectiveness of Its Program

GAO 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.

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.