GAO

Accountability•Integrity•Reliability

Highlights

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

August 2007

INFORMATION SECURITY

Selected Departments Need to Address Challenges in Implementing Statutory Requirements

Why GAO Did This Study

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

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

What GAO Recommends

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

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

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

What GAO Found

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

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

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

Security Requirements That Challenge Selected Departments

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

Source: GAO.