February 28, 2007

INFORMATION SECURITY

Veterans Affairs Needs to Address Long-Standing Weaknesses

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-532T a testimony before the Subcommittee on Oversight and Investigations of the House Committee on Veterans' Affairs.

Why GAO Did This Study

Security breaches at the Department of Veterans Affairs (VA) and other public and private organizations have highlighted the importance of well-designed and implemented information security programs. GAO was asked to testify on its past work on VA's information security program, as well as ongoing reviews that it is conducting at VA.

In developing its testimony, GAO drew on over 15 of its previous reports and testimonies, as well as reports by the department's inspector general (IG).

What GAO Recommends

To ensure that security issues are adequately addressed, GAO has previously made over 150 recommendations to VA on implementing effective controls and developing a robust information security program.

www.gao.gov/cgi-bin/getrpt?GAO-07-532T

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

What GAO Found

For many years, GAO has raised significant concerns about VA's information security—particularly its lack of a comprehensive information security program, which is vital to safeguarding government information. The figure below details information security weaknesses that GAO identified from 1998 to 2005. As shown, VA had not consistently implemented appropriate controls for (1) limiting, preventing, and detecting electronic access to sensitive computerized information; (2) restricting physical access to computer and network equipment to authorized individuals; (3) segregating incompatible duties among separate groups or individuals; (4) ensuring that changes to computer software were authorized and timely; or (5) providing continuity of computerized systems and operations. The department's IG has also reported recurring weaknesses throughout VA in such areas as access controls, physical security, and segregation of incompatible duties. In response, the department has taken actions to address these weaknesses, but these have not been sufficient to establish a comprehensive information security programs. As a result, sensitive information has remained vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure. Without an established and implemented security program, the department will continue to have major challenges in protecting its systems and information from security breaches.

GAO has several ongoing engagements to review the department's efforts in improving its information security and information technology management. These engagements address:

- data breach notification;
- actions to strengthen information security controls;
- controls over information technology equipment; and
- VA's information technology realignment effort.

Figure: Chronology of Information Security Weaknesses Identified by GAO

		Information security control areas					
Year	VA location or agency	Access control	Physical security	Segregation of duties	Change control	Service continuity	Security program
1998	Austin	●	●	●	●	●	●
	Dallas	●	●			●	●
	Albuquerque	●	●	●		●	●
	Hines	●					●
	Philadelphia	●					●
1999	Austin	●			●		●
2000	Maryland	●	●	●	●	●	●
	New Mexico	●	●	●	●	●	●
	North Texas/Dallas	●	●	●		●	●
2000	Departmentwide	●		●			●
2002	Departmentwide						●
2005	Departmentwide	●	●	●	●	●	●

● Weakness found in this area

■ Control area not included in scope of audit

Source: GAO reports.

Note: Hines is a suburb of Chicago.