GAO

Accountability·Integrity·Reliability

Highlights

Highlights of GAO-10-727T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, U.S. House of Representatives

Why GAO Did This Study

Since 1997, GAO has identified information security as a governmentwide high-risk issue. This has been particularly true at the Department of Veterans Affairs (VA), where the department has been challenged in protecting the availability, confidentiality, and integrity of its information and systems. Since the 1990s, GAO has highlighted the challenges the department has faced, including the need to safeguard personal information.

GAO was asked to testify on VA's progress in implementing information security and the department's compliance with the Federal Information Security Management Act of 2002 (FISMA), a comprehensive framework for securing federal information resources. In preparing this testimony, GAO analyzed prior GAO, Office of Management and Budget, VA Office of Inspector General, and VA reports related to the department's information security program.

What GAO Recommends

In previous reports over the past several years, GAO has made numerous recommendations to VA aimed at improving the effectiveness of the department's efforts to strengthen information security practices and to ensure that security issues are adequately addressed.

View GAO-10-727T or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Valerie C. Melvin at (202) 512-6304 or melvinv@gao.gov.

May 19, 2010

INFORMATION SECURITY

Veterans Affairs Needs to Resolve Long-Standing Weaknesses

What GAO Found

VA has made limited progress in resolving long-standing deficiencies in securing its information and systems. In September 2007 and also March 2010, GAO reported that VA had begun or had continued work on several initiatives to strengthen information security practices, but that shortcomings in the implementation of those initiatives could limit their effectiveness. VA has also consistently had weaknesses in major information security control areas. As shown in the table below, VA was deficient in each of five major categories of information security controls as defined in the GAO *Federal Information System Controls Audit Manual*.

Control Weaknesses for Fiscal Years 2006 - 2009

Security Control Category	2006	2007	2008	2009
Access control	●	●	●	●
Configuration management	●	●	●	●
Segregation of duties	●	●	●	●
Contingency planning	●	●	●	●
Security management	●	●	●	●

Source: GAO analysis based on VA and Inspector General reports.

Further, in VA's fiscal year 2009 performance and accountability report, the independent auditor stated that, while VA continued to make progress, IT security and control weaknesses remained pervasive and continued to place VA's program and financial data at risk. The independent auditor also noted that VA's controls over its financial systems constituted a material weakness (a significant deficiency that can result in an undetected material misstatement of the department's financial statements.)

Since 2006, VA's progress in fully implementing the information security program required under FISMA has been mixed. For example, from 2006 to 2009, the department reported a dramatic increase in the percentage of systems for which a contingency plan was tested. However, during the same period, the department reported a decrease in the percentage of employees who had received security awareness training.

Until VA fully and effectively implements a comprehensive information security program and mitigates known security vulnerabilities, its computer systems and sensitive information (including personal information of veterans and their beneficiaries) will remain exposed to an unnecessary and increased risk of unauthorized use, disclosure, tampering, theft, and destruction.