G A O
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-07-1019, a report to congressional requesters

September 2007

INFORMATION SECURITY

Sustained Management Commitment and Oversight Are Vital to Resolving Long-standing Weaknesses at the Department of Veterans Affairs

Why GAO Did This Study

In May 2006, the Department of Veterans Affairs (VA) announced that computer equipment containing personal information on approximately 26.5 million veterans and active duty military personnel had been stolen. Given the importance of information technology (IT) to VA's mission, effective information security controls are critical to maintaining public and veteran confidence in its ability to protect sensitive information. GAO was asked to evaluate (1) whether VA has effectively addressed GAO and VA Office of Inspector General (IG) information security recommendations and (2) actions VA has taken since May 2006 to strengthen its information security practices and secure personal information. To do this, GAO examined security policies and action plans, interviewed pertinent department officials, and conducted testing of encryption software at select VA facilities.

What GAO Recommends

GAO is making 17 recommendations to the Secretary of Veterans Affairs aimed at improving the effectiveness of VA's efforts to strengthen information security practices by developing and documenting processes, policies, and procedures, and completing the implementation of key initiatives. In commenting on a draft of this report, VA stated that it generally agreed with the recommendations and has implemented or is working to implement them.

www.gao.gov/cgi-bin/getrpt?GAO-07-1019.

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

What GAO Found

Although VA has made progress, it has not yet fully implemented most of the key GAO and IG recommendations to strengthen its information security practices. Specifically, VA has implemented two GAO recommendations: to develop a process for managing its plan to correct identified weaknesses and to regularly report on progress in updating its security plan to the Secretary. However, it has not fully implemented two other GAO recommendations: to complete a comprehensive security management program and to ensure consistent use of information security performance standards for appraising senior VA executives. In addition, the department has not yet fully implemented 20 of 22 recommendations made by the IG in 2006. For example, VA has not completed activities to appropriately restrict access to data, networks, and department facilities; ensure that only authorized changes and updates to computer programs are made; and strengthen critical infrastructure planning. Because these recommendations have not yet been implemented, unnecessary risk exists that the personal information of veterans and others, such as medical providers, will be exposed to data tampering, fraud, and inappropriate disclosure.

Since the May 2006 security incident, VA has continued or begun several major initiatives to strengthen its information security practices and secure personal information within the department, but more remains to be done. These initiatives include continuing efforts begun in October 2005 to reorganize its management structure to provide better oversight and fiscal discipline over its IT systems; developing an action plan to correct identified weaknesses; establishing an information protection program; improving its incident management capability; and establishing an office responsible for oversight of IT within the department. However, implementation shortcomings limit the effectiveness of these initiatives. For example, no documented process exists between the Director of Field Operations and Security and the chief information security officer (CISO) to ensure the effective coordination and implementation of security policies and procedures within the department. In addition, the position of the CISO has been unfilled since June 2006. Although, 39 percent of items in the department's remedial action plan are tasks to develop, document, revise, or update a policy or program, 87 percent of these items have no corresponding task with an established time frame for implementation across the department. VA also did not have clear guidance for identifying devices that require encryption functionality, and it lacked adequate procedures for incident response and notification. Finally, VA's Office of IT Oversight and Compliance lacks a standard methodology and established criteria to ensure that its examination of internal controls is consistent across VA facilities. Until the department addresses recommendations to resolve identified weaknesses and implements the major initiatives it has undertaken, it will have limited assurance that it can protect its systems and information from the unauthorized disclosure, misuse, or loss of personal information of veterans and other personnel.