June 14, 2006

VETERANS AFFAIRS

Leadership Needed to Address Information Security Weaknesses and Privacy Issues

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-866T, a testimony before the Committee on Veterans' Affairs, House of Representatives

Why GAO Did This Study

The recent information security breach at the Department of Veterans Affairs (VA), in which personal data on millions of veterans were compromised, has highlighted the importance of the department's security weaknesses, as well as the ability of federal agencies to protect personal information. Robust federal security programs are critically important to properly protect this information and the privacy of individuals.

GAO was asked to testify on VA's information security program, ways that agencies can prevent improper disclosures of personal information, and issues concerning notifications of privacy breaches. In preparing this testimony, GAO drew on its previous reports and testimonies, as well as on expert opinion provided in congressional testimony and other sources.

What GAO Recommends

To ensure that security and privacy issues are adequately addressed, GAO has made recommendations previously to VA and other agencies on implementing federal privacy and security laws. In addition, GAO has previously testified that in considering security breach notification legislation, the Congress should consider setting specific reporting requirements for agencies.

www.gao.gov/cgi-bin/getrpt?GAO-06-866T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

For many years, significant concerns have been raised about VA's information security—particularly its lack of a robust information security program, which is vital to avoiding the compromise of government information, including sensitive personal information. Both GAO and the department's inspector general have reported recurring weaknesses in such areas as access controls, physical security, and segregation of incompatible duties. The department has taken steps to address these weaknesses, but these have not been sufficient to establish a comprehensive information security program. For example, it is still developing plans to complete a security incident response program to monitor suspicious activity and cyber alerts, events, and incidents. Without an established and implemented security program, the department will continue to have major challenges in protecting its information and information systems from security breaches such as the one it recently experienced.

In addition to establishing robust security programs, agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised. A key step is to develop a privacy impact assessment—an analysis of how personal information is collected, stored, shared, and managed—whenever information technology is used to process personal information. In addition, agencies can take more specific practical measures aimed at preventing data breaches, including limiting the collection of personal information, limiting the time that such data are retained, limiting access to personal information and training personnel accordingly, and considering the use of technological controls such as encryption when data need to be stored on portable devices.

When data breaches do occur, notification of those affected and/or the public has clear benefits, allowing people the opportunity to protect themselves from identity theft. Although existing laws do not require agencies to notify the public of data breaches, such notification is consistent with agencies' responsibility to inform individuals about how their information is being accessed and used, and it promotes accountability for privacy protection. That said, care is needed in defining appropriate criteria for triggering notification. Notices should be coordinated with law enforcement to avoid impeding ongoing investigations, and in order to be effective, notices should be easy to understand. Because of the possible adverse impact of a compromise of personal information, it is critical that people fully understand the threat and their options for addressing it.

Strong leadership, sustained management commitment and effort, disciplined processes, and consistent oversight will be needed for VA to address its persistent, long-standing control weaknesses.