United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

For Release on Delivery
Expected at time 2:00 p.m. EST
February 28, 2007

INFORMATION SECURITY

Veterans Affairs Needs to Address Long-Standing Weaknesses

Statement of Gregory C. Wilshusen
Director, Information Security Issues

Accountability * Integrity * Reliability

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.

February 28, 2007

INFORMATION SECURITY

Veterans Affairs Needs to Address Long-Standing Weaknesses

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.

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on information security management at the Department of Veterans Affairs (VA). For many years, GAO has identified information security as a governmentwide high-risk issue[1] and emphasized its criticality for protecting the government's information assets. GAO has issued over 15 reports and testimonies and made over 150 recommendations from 1998 to 2005 related to VA's information security program.

Today I will address VA's information security management, including weaknesses that GAO and others have reported, as well as actions that the department has taken to resolve these deficiencies. I will also discuss ongoing audit work that GAO is conducting at VA.

To describe VA's information security management, we reviewed our previous work in this area, as well as reports by the department and its Office of Inspector General (IG). To provide additional context, we have included, as an attachment, a list of key GAO publications related to VA security issues. All GAO work conducted for this testimony is in accordance with generally accepted government auditing standards.

Results in Brief

Significant concerns have been raised over the years about VA's information security—particularly its lack of a robust information security program, which is vital to avoiding the compromise of government information. We have previously reported on wide-ranging deficiencies in VA's information security controls.[2] For example, VA had not consistently implemented appropriate controls

[1] GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007); *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005).

[2] See attachment 1.

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 changes to computer software were authorized and timely; and (5) providing continuity of computerized systems and operations. The department's IG has recently identified similar weaknesses. These long-standing deficiencies existed, in part, because VA had not implemented key components of a comprehensive, integrated information security program. Although the department has taken steps to implement components of its security program, its efforts have not been sufficient to effectively protect its information and information systems. As a result, sensitive information remains vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure.

We have several ongoing engagements to perform work at VA to review the department's efforts in improving its information security and information technology management. Our ongoing work is examining data breach notification, actions to strengthen information security controls, controls over information technology equipment, and implementation of an information technology realignment initiative.

Background

Information security is a critical consideration for any organization that depends on information systems and networks to carry out its mission or business. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and the inappropriate disclosure of sensitive information. Recognizing the importance of securing federal systems and data, Congress passed the Federal Information Security Management Act (FISMA) in 2002, which set forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.[3]

Under FISMA, agencies are required to provide sufficient safeguards to cost-effectively protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure. The act requires each agency to develop, document, and implement an agencywide information security program that is to include assessing risk; developing and implementing policies, procedures, and security plans; providing security awareness and training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial action to address information security deficiencies; detecting, reporting, and responding to security incidents; and ensuring continuity of operations.

In providing health care and other benefits to veterans and their dependents, VA relies on a vast array of computer systems and telecommunications networks to support its operations and store sensitive information, including personal information on veterans. Effectively securing these computer systems and networks is critical to the department's ability to safeguard its assets and sensitive information.

VA's Information Security Weaknesses Are Long Standing

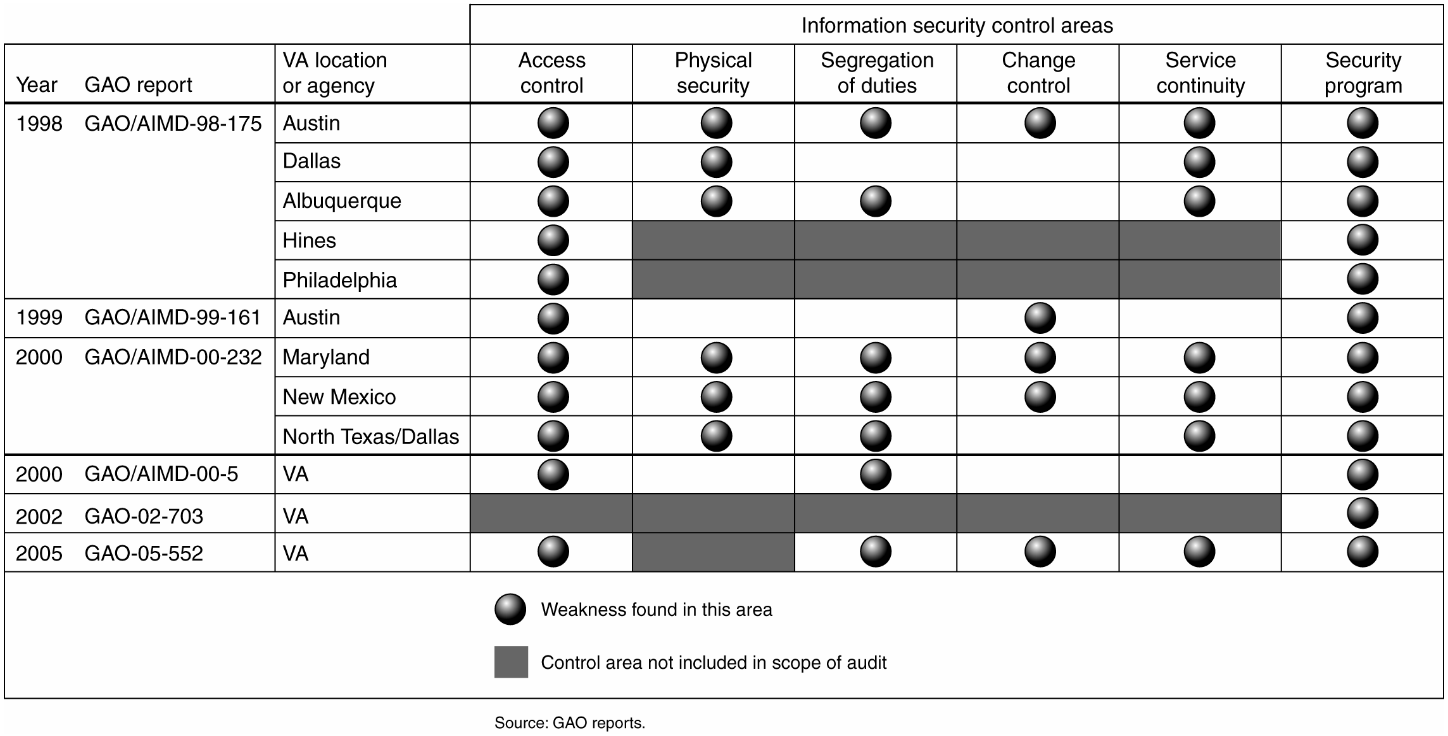
VA has faced long-standing challenges in achieving effective information security across the department. Our previous reports and testimonies[4] have identified wide-ranging, often recurring deficiencies in the department's information security controls. For example, VA had not consistently implemented appropriate controls for (1) limiting, preventing, and detecting electronic access to

[3] FISMA, Title III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002).

[4] Attachment 1 includes a list of our products related to information technology vulnerabilities at VA.

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 changes to computer software were authorized and timely; and (5) providing continuity of computerized systems and operations. Figure 1 details the information security control weaknesses we identified at VA from 1998 through 2005.

Figure 1: Chronology of Information Security Weaknesses Identified by GAO



			Information security control areas					
Year	GAO report	VA location or agency	Access control	Physical security	Segregation of duties	Change control	Service continuity	Security program
1998	GAO/AIMD-98-175	Austin	●	●	●	●	●	●
		Dallas	●	●			●	●
		Albuquerque	●	●	●		●	●
		Hines	●	▨	▨	▨	▨	●
		Philadelphia	●	▨	▨	▨	▨	●
1999	GAO/AIMD-99-161	Austin	●			●		●
2000	GAO/AIMD-00-232	Maryland	●	●	●	●	●	●
		New Mexico	●	●	●	●	●	●
		North Texas/Dallas	●	●	●		●	●
2000	GAO/AIMD-00-5	VA	●		●			●
2002	GAO-02-703	VA	▨	▨	▨	▨	▨	●
2005	GAO-05-552	VA	●	▨	●	●	●	●

● Weakness found in this area

▨ Control area not included in scope of audit

Source: GAO reports.

Notes: Hines is a suburb of Chicago.

Full citations are provided in attachment 1.

These weaknesses existed, in part, because VA had not implemented key components of a comprehensive information security program. Specifically, VA's information security efforts lacked

- clearly delineated security roles and responsibilities;
- regular, periodic assessments of risk;

- security policies and procedures that addressed all aspects of VA's interconnected environment;
- an ongoing security monitoring program to identify and investigate unauthorized, unusual, or suspicious access activity; and
- a process to measure, test, and report on the continued effectiveness of computer system, network, and process controls.

We made a number of recommendations in 2002 that were aimed at improving VA's security management.[5] Among the primary elements of these recommendations were that VA centralize its security management functions and perform other actions to establish an information security program, including actions related to risk assessments, security policies and procedures, security awareness, and monitoring and evaluating computer controls.[6]

Since our report in 2002, VA's independent auditors and its IG have continued to report serious weaknesses with the department's information security controls. In the auditors' report on internal controls prepared at the completion of VA's 2006 financial statement audit, information technology security controls were identified as a material weakness because of serious weaknesses related to access control, segregation of duties, change control, and service continuity.[7] These areas of weakness are virtually identical to those that we had identified years earlier.

[5] GAO, *Veterans Affairs: Sustained Management Attention Is Key to Achieving Information Technology Results*, GAO-02-703 (Washington, D.C.: June 12, 2002).

[6] We based our recommendations on guidance and practices provided in GAO, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999); *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998); *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D. C.: November 1999); and Chief Information Officer Council, *Federal Information Technology Security Assessment Framework* (Washington, D.C.: Nov. 28, 2000). The provisions of FISMA (passed in late 2002) and associated guidance were generally consistent with this earlier guidance.

[7] The auditor's report is included in VA's *FY 2006 Annual Performance and Accountability Report.*

The department's *FY 2006 Annual Performance and Accountability Report* states that the IG continues to identify the same vulnerabilities and make the same recommendations year after year. The IG's September 2006 audit of VA's information security program noted that 16 previously reported recommendations remained unimplemented; it also identified a new weakness and made an additional recommendation. The IG has reported information technology security as a major management challenge for the department each year for the past 6 years.

VA's Efforts to Address Information Security Weaknesses Have Been Limited

Despite having taken steps to address the weaknesses described in our earlier work, VA has not yet resolved these weaknesses on a departmentwide basis or implemented a comprehensive information security program.[8] For example:

- *Central security management function*: In October 2006, the department moved to a centralized management model. The department has also contracted for project support in helping to frame a security governance structure and provide tools to assist management with controls over information technology assets. This work is scheduled to be completed in March 2007.
- *Periodic risk assessments:* VA is implementing a commercial tool to identify the level of risk associated with system changes and also to conduct information security risk assessments. It also created a methodology that establishes minimum requirements for such risk assessments. However, it has not yet completed its risk assessment policy and guidance. While the policy and guidance were originally scheduled to be completed by the end of 2006, the completion date was extended to April 2007.
- *Security policies and procedures:* VA is in the process of developing policies and directives to strengthen security controls as part of its action plan. For example, VA planned to

[8] This result is also reflected in the department's failing grade in the annual report card on computer security that was issued by the then House Committee on Government Reform: *Computer Security Report Card* (Washington, D.C.: Mar. 16, 2006).

develop directives by the end of 2006 on access controls and media protection, standards for restricting use of portable and mobile devices, and policies regarding physical access to VA computer rooms. However, the completion date for development of these policies has been extended to April 2007.

- *Security awareness:* VA has taken steps to improve security awareness training. It holds an annual department information security conference, and it has developed a Web portal for security training, policy, and procedures, as well as a security awareness course that VA employees are required to review annually. However, VA has not demonstrated that it has a process to ensure compliance.
- *Monitoring and evaluating computer controls:* VA has taken steps to improve the monitoring and evaluating of computer controls by developing policies and procedures. For example, VA planned to develop by the end of 2006 criteria for system security control testing at least every 3 years and planned to identify key system security controls for testing on a routine basis. However, the completion dates for development of these policies have been extended to April 2007.

To fulfill our recommendations in these areas, VA must not only complete and document the policies, procedures, and plans that it is currently developing, but also implement them effectively. With regard to its IG's findings and recommendations, the department has established an action plan to address the material weakness in information security (Data Security—Assessment and Strengthening of Controls), which is to correct deficiencies and eliminate vulnerabilities in this area. Despite these actions, the department has not implemented the key elements of a comprehensive security management program, and its efforts have not been sufficient to effectively protect its information systems and information, including personal information, from unauthorized disclosure, misuse, or loss.

GAO Has Ongoing Reviews of Information Technology and Security Issues at VA

We have several ongoing engagements to perform work at VA to review the department's efforts in improving its information security and information technology management. These engagements address:

- *Data breach notification:* We are conducting a study to determine the lessons that can be learned from the VA data breach with respect to notifying government officials and affected individuals about data breaches. For this evaluation, we are examining similar data breach cases at other federal agencies, as well as analyzing federal guidance on data breach notification procedures.
- *Actions to strengthen information security controls*: We are conducting a review to evaluate VA's efforts to implement prior GAO and IG information security-related recommendations and to assess actions VA has taken since the data breach of May 3, 2006, to strengthen information security and protect personal information. As part of this engagement, we are examining VA's time line of planned efforts to strengthen controls.
- *Controls over information technology equipment*: We are conducting a follow-up audit[9] at selected VA locations to determine the risk of theft, loss, or misappropriation of information technology equipment. To perform our audit, we are assessing the effectiveness of physical inventory controls and the property disposal process at four VA locations.
- *VA's information technology realignment initiative:* We are conducting a review to determine whether VA's realignment plan for its Office of Information and Technology includes critical factors for successful implementation of a centralized management model. We are also looking at how the realignment will ensure that under the centralized management approach,

[9] This is a follow-up audit to work reported in GAO, *VA Medical Centers: Internal Control Over Selected Operating Functions Needs Improvement*, GAO-04-755 (Washington, D.C.: July 21, 2004).

the chief information officer is accountable for the entire information technology budget (including those funds that had been administered by the Veterans Health Administration and Veterans Benefits Administration). In performing this evaluation, we are analyzing governance and implementation plans, as well as budgetary and other relevant documentation.

In summary, long-standing information security control weaknesses at VA have placed its information systems and information at increased risk of misuse and unauthorized disclosure. Although VA has taken steps to mitigate previously reported weaknesses, the department has not yet resolved these weaknesses, implemented the recommendations of GAO and the IG, or implemented a comprehensive information security program, which it needs in order to effectively manage risks on an ongoing basis. Much work remains to be done. Only through strong leadership, sustained management commitment and effort, disciplined processes, and consistent oversight can VA address its persistent, long-standing control weaknesses.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other members of the subcommittee may have.

Contact and Acknowledgments

If you have any questions concerning this statement, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244, wilshuseng@gao.gov. Other individuals who made key contributions include Barbara Collier, Mary Hatcher, Valerie Hopkins, Leena Mathew, and Charles Vrabel.

Attachment 1: Selected GAO Products

Information Security: Leadership Needed to Address Weaknesses and Privacy at Veterans Affairs. GAO-06-897T. Washington, D.C.: June 20, 2006.

Veterans Affairs: Leadership Needed to Address Security Weaknesses and Privacy Issues. GAO-06-866T. Washington, D.C.: June 14, 2006.

Privacy: Preventing and Responding to Improper Disclosures of Personal Information. GAO-06-833T. Washington, D.C.: June 8, 2006.

Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements. GAO-05-552. Washington, D.C.: July 15, 2005.

Veterans Affairs: Sustained Management Attention is Key to Achieving Information Technology Results. GAO-02-703. Washington, D.C.: June 12, 2002.

Major Management Challenges and Program Risks: Department of Veterans Affairs. GAO-01-255. Washington, D.C.: January 2001.

VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration. GAO/AIMD-00-232. Washington, D.C.: September 8, 2000.

Information Systems: The Status of Computer Security at the Department of Veterans Affairs. GAO/AIMD-00-5. Washington, D.C.: October 4, 1999.

VA Information Systems: The Austin Automation Center Has Made Progress in Improving Information System Controls. GAO/AIMD-99-161. Washington, D.C.: June 8, 1999.

Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure. GAO/AIMD-98-175. Washington, D.C.: September 23, 1998.

(310591)

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER