United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, U.S. House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, May 19, 2010

INFORMATION SECURITY

Veterans Affairs Needs to Resolve Long-Standing Weaknesses

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

Valerie C. Melvin,
Director, Information Management and Human Capital Issues

May 19, 2010

INFORMATION SECURITY

Veterans Affairs Needs to Resolve Long-Standing Weaknesses

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.

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.

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to participate in today's hearing on information security at the Department of Veterans Affairs (VA). Since 1997, we have identified information security as a governmentwide high-risk issue and emphasized its importance in protecting the availability, confidentiality, and integrity of the information residing on federal information systems.[1] Since the 1990s, we have highlighted challenges the department has faced, including the need to safeguard personal information.

In our testimony today, we will discuss VA's progress in implementing information security and the department's compliance with the Federal Information Security Management Act of 2002 (FISMA).[2] In preparing this testimony, we analyzed prior GAO, Office of Management and Budget (OMB), VA Office of Inspector General (OIG), and VA reports related to the department's information security program for fiscal years 2006 through 2009. We conducted our review from April to May 2010 in the Washington, D.C., area in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives.

Background

VA's mission is to promote the health, welfare, and dignity of all veterans in recognition of their service to the nation by ensuring that they receive medical care, benefits, social support, and memorials. According to recent information from the Department of Veterans Affairs, its employees maintain the largest integrated health care system in the nation for more than 5.6 million patients, provide compensation and pension benefits for nearly 4 million veterans and beneficiaries, and maintain nearly 3 million gravesites at 163 properties. The use of IT is crucial to the department's ability to provide these benefits and services, but without adequate

[1]GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009) and *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses*, GAO-09-546 (Washington, D.C.: July 17, 2009).

[2]FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

protections, VA's systems and information are vulnerable to those with malicious intentions who wish to exploit the information.

To help protect against threats to federal systems, FISMA sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. The framework creates a cycle of risk management activities necessary for an effective security program. In order to ensure the implementation of this framework, FISMA assigns responsibilities to OMB that include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and reviewing and approving or disapproving agency information security programs, at least annually. It also assigns specific responsibilities to agency heads, chief information officers, inspectors general, and the National Institute of Standards and Technology (NIST), in particular requiring chief information officers and inspectors general to submit annual reports to OMB.

In addition, Congress enacted the Veterans Benefits, Health Care, and Information Technology Act of 2006,[3] after a serious loss of data earlier that year revealed weaknesses in VA's handling of personal information. Under the act, VA's Chief Information Officer is responsible for establishing, maintaining, and monitoring departmentwide information security policies, procedures, control techniques, training, and inspection requirements as elements of the department's information security program. It also reinforced the need for VA to establish and carry out the responsibilities outlined in FISMA, and included provisions to further protect veterans and service members from the misuse of their sensitive personal information and to inform Congress regarding security incidents involving the loss of that information.

[3]Veterans Benefits, Health Care, and Information Technology Act of 2006, Pub. L. No. 109-461, 120 Stat. 3403, 3450 (Dec. 22, 2006).

VA Has Made Limited Progress in Addressing Information Security Weaknesses

For over a decade, VA has faced long-standing information security weaknesses as identified by GAO, the VA's OIG, and by the department itself. These weaknesses have left VA vulnerable to disruptions in critical operations, theft, fraud, and inappropriate disclosure of sensitive information. VA's efforts to address these deficiencies have had limited progress to date.

In September 2007, we reported that VA had begun or had continued several initiatives to strengthen information security practices within the department, but that shortcomings with the implementation of those initiatives could limit their effectiveness.[4] At that time, we made 17 recommendations for improving the department's information security practices. We verified that VA had implemented five of those recommendations, including developing guidance for the information security program and documenting related responsibilities. VA has efforts under way to address 11 of the remaining 12 recommendations. These efforts include ensuring remedial action items are completed in an effective and timely manner, implementing guidance on encryption, and developing and documenting procedures to obtain contact information for individuals whose personal information has been compromised in a security breach. We plan to assess whether the department's actions substantially implement these 11 recommendations, and whether VA is now taking action on the twelfth recommendation to maintain an accurate inventory of all IT equipment that has encryption installed.

In March 2010, we reported[5] that federal agencies, including VA, had made limited progress in implementing the Federal Desktop Core Configuration (FDCC) initiative to standardize settings on workstations.[6] We determined that VA had implemented certain requirements of the initiative, such as

[4]GAO, *Information Security: Sustained Management Commitment and Oversight Are Vital to Resolving Long-standing Weaknesses at the Department of Veterans Affairs*, GAO-07-1019 (Washington, D.C.: Sep. 7, 2007).

[5]GAO, *Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements*, GAO-10-202 (Washington, D.C.: March 12, 2010).

[6]In March 2007 the Office of Management and Budget (OMB) launched the Federal Desktop Core Configuration initiative to standardize and strengthen information security at federal agencies. Under the initiative agencies were to implement a standardized set of configuration settings on workstations with Microsoft Windows XP or Vista operating systems. OMB intended that by implementing the initiative, agencies would establish a baseline level of information security, reduce threats and vulnerabilities, and improve protection of information and related assets.

documenting deviations from the standardized set of configuration settings for Windows workstations and putting a policy in place to officially approve these deviations. However, VA had not fully implemented several key requirements. For example, the department had not included language in contracts to ensure that new acquisitions address the settings and that products of IT providers operate effectively using them. Additionally, VA had not obtained a NIST-validated tool to monitor implementation of standardized workstation configuration settings. To improve the department's implementation of the initiative, we made four recommendations: (1) complete implementation of VA's baseline set of configuration settings, (2) acquire and deploy a tool to monitor compliance with FDCC, (3) develop, document, and implement a policy to monitor compliance, and (4) ensure that FDCC settings are included in new acquisitions and that products operate effectively using these settings. VA concurred with all of our recommendations and indicated that it plans to implement them by September 2010.

VA Continues to Report Significant Information Security Shortcomings

Information security remains a long-standing challenge for the department. In 2009, for the 13th year in a row, VA's independent auditor reported that inadequate information system controls over financial systems constituted a material weakness.[7] Among 24 major federal agencies, VA was one of six agencies in fiscal year 2009 to report such a material weakness.

VA's independent auditor stated that while the department continued to make steady progress, IT security and control weaknesses remained pervasive and placed VA's program and financial data at risk. The auditor noted the following weaknesses:

- Passwords for key VA network domains and financial applications were not consistently configured to comply with agency policy.
- Testing of contingency plans for financial management systems at selected facilities was not routinely performed and documented to meet the requirements of VA policy.

[7]A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

- Many IT security control deficiencies were not analyzed and remediated across the agency and a large backlog of deficiencies remained in the VA plan of action and milestones system. In addition, previous plans of action and milestones were closed without sufficient and documented support for the closure.

In addition, VA has consistently had weaknesses in major information security control areas. As shown in table 1, for fiscal years 2006 through 2009, deficiencies were reported in each of the five major categories of information security controls[8] as defined in our *Federal Information System Controls Audit Manual.*[9]

Table 1: 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.

In fiscal year 2009, for the 10th year in a row, the VA OIG designated VA's information security program and system security controls as a major management challenge for the department. Of 24 major federal agencies, the department was 1 of 20 to have information security designated as a major management challenge. The OIG noted that the department had made progress in implementing components of an agencywide information security program, but nevertheless continued to identify major IT security deficiencies in the annual information security program audits. To assist the department in improving its information security, the OIG made

[8]Access controls ensure that only authorized individuals can read, alter, or delete data; configuration management controls provide assurance that only authorized software programs are implemented; segregation of duties reduces the risk that one individual can independently perform inappropriate actions without detection; continuity of operations planning provides for the prevention of significant disruptions of computer-dependent operations; and an agencywide information security program provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

[9]GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: Feb. 2009).

recommendations for strengthening access controls, configuration management, change management, and service continuity. Effective implementation of these recommendations could help VA to prevent, limit, and detect unauthorized access to computerized networks and systems and help ensure that only authorized individuals can read, alter, or delete data.

The need to implement effective security is clear given the history of security incidents at the department. VA has reported an increasing number of security incidents and events over the last few years. Each year during fiscal years 2007 through 2009, the department reported a higher number of incidents and the highest number of incidents in comparison to 23 other major federal agencies.

VA's Uneven Implementation of FISMA Limits the Effectiveness of Security Efforts

FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. As part of its oversight responsibilities, OMB requires agencies to report on specific performance measures, including the percentage of:

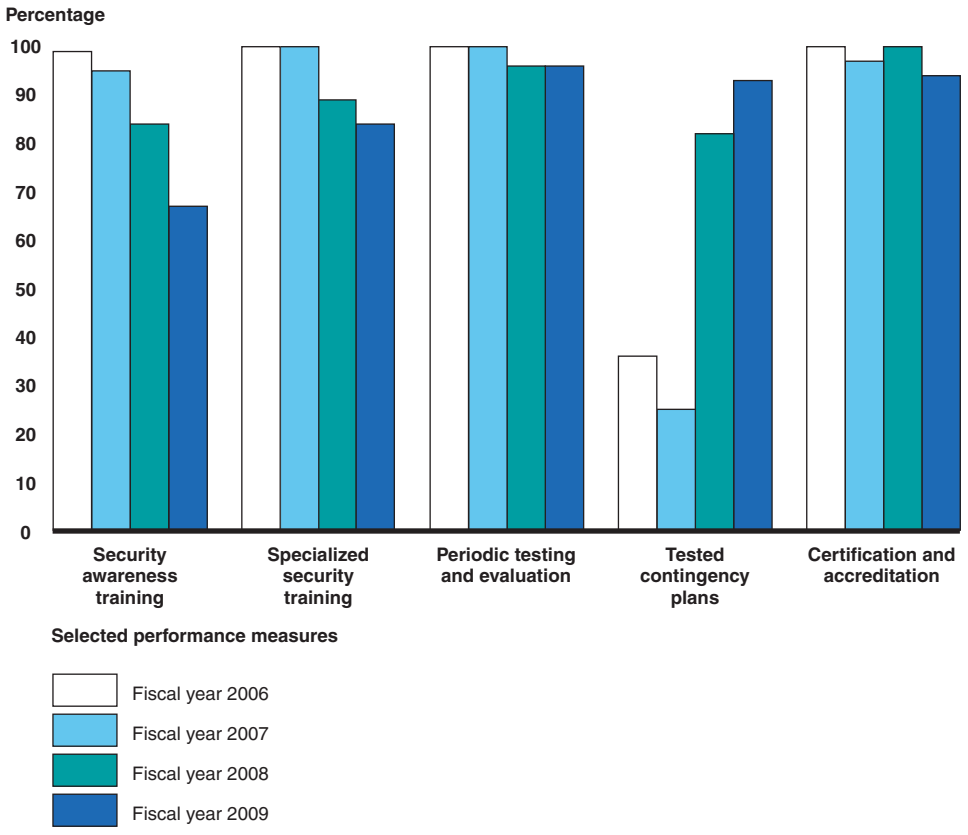
- employees and contractors receiving IT security awareness training, and those who have significant security responsibilities and have received specialized security training,
- systems whose controls were tested and evaluated, have tested contingency plans, and are certified and accredited.[10]

Since fiscal year 2006, VA's progress in fully implementing the information security program required under FISMA and following the policies issued by OMB has been mixed. For example, from 2006 to 2009, the department has reported a dramatic increase in the percentage of systems for which a

[10]Certification is a comprehensive assessment of management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision to authorize operation of an information system and to explicitly accept the risk to agency operations based on implementation of controls.

contingency plan was tested in accordance with OMB policy. However, during the same period, it reported decreases in both the percentage of employees who had received security awareness training and the percentage of employees with significant security responsibilities who had received specialized security training (see fig. 1). These decreases in the percentage of individuals who had received information security training could limit the ability of VA to effectively implement security measures.

Figure 1: VA Key Performance Measures for Fiscal Years 2006 - 2009

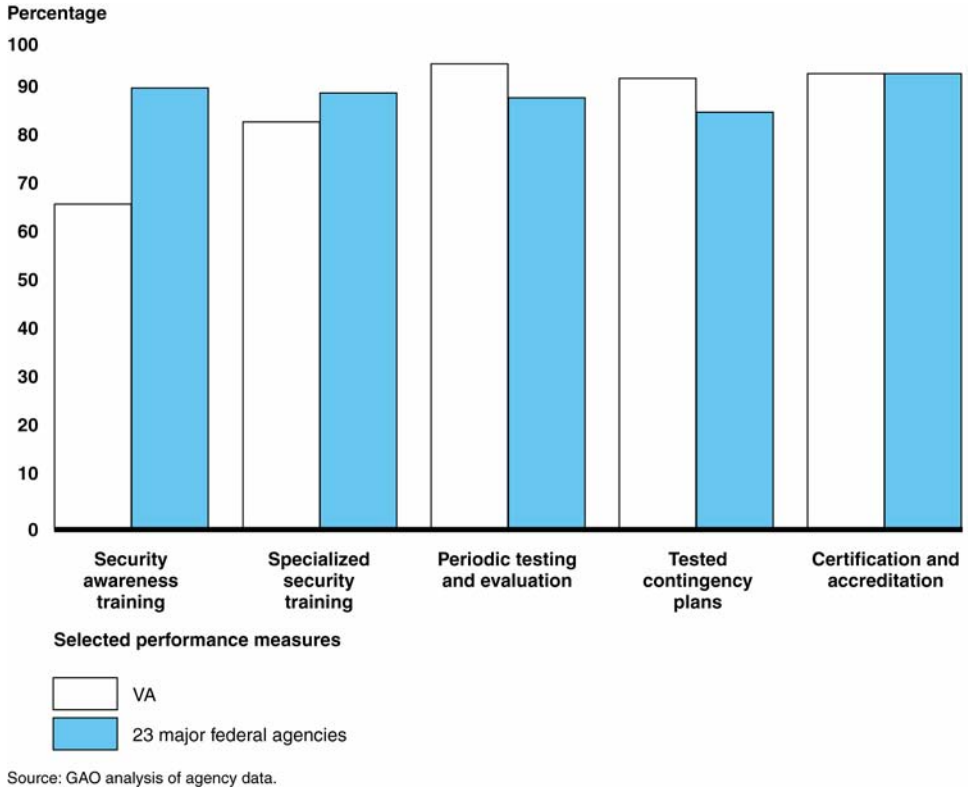


Source: GAO analysis of agency data.

For fiscal year 2009, in comparison to 23 other major federal agencies, VA's efforts to implement these information security control activities were equal to or higher in some areas and lower in others. For example, VA reported equal or higher percentages than other federal agencies in the number of systems for which security controls had been tested and reviewed in the past year, the number of systems for which contingency plans had been tested in accordance with OMB policy, and the number of

systems that had been certified and accredited. However, VA reported lower percentages of individuals who received security awareness training and lower percentages of individuals with significant security responsibilities who received specialized security training (see fig. 2).

Figure 2: Comparison VA to Governmentwide Performance for Fiscal Year 2009



Source: GAO analysis of agency data.

In summary, effective information security controls are essential to securing the information systems and information on which VA depends to carry out its mission. The department continues to face challenges in resolving long-standing weaknesses in its information security controls and in fully implementing the information security program required under FISMA. Overcoming these challenges will require sustained leadership, management commitment, and effective oversight. 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.

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

Contacts 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, or Valerie C. Melvin, Director, Information Management and Human Capital Issues, at (202) 512-6304, melvinv@gao.gov. Other individuals who made key contributions include Charles Vrabel and Anjalique Lawrence (assistant directors), Nancy Glover, Mary Marshall, and Jayne Wilson.

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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

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

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548