United States Government Accountability Office

GAO

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

G A O

Accountability * Integrity * Reliability

GAO
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.

Contents

Tables

Figure

Abbreviations

CIO	chief information officer
CISO	chief information security officer
FISMA	Federal Information Security Management Act
NSOC	Network and Security Operations Center
IG	Inspector General
IT	information technology
ITOC	VA's Office of Information Technology Oversight and Compliance
OMB	Office of Management and Budget
US-CERT	United States Computer Emergency Readiness Team
VA	Department of Veterans Affairs
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 7, 2007

Congressional Requesters

The mission of the Department of Veterans Affairs (VA) 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 lasting memorials. In providing health care and other benefits to veterans and their dependents, the department relies on a vast array of computer systems and telecommunications networks to support its operations and store sensitive information, including personal information on veterans.

Given the importance of information technology for supporting VA's mission—the department expended $1.2 billion in fiscal year 2006 on information technology (IT)—successfully securing these systems with effective information security controls is critical to the department's ability to safeguard its assets and sensitive information.[1] To assist the department in improving its information security program, we and the VA Office of Inspector General (IG) have previously recommended that VA take steps to improve its security management program, including actions to improve controls to appropriately restrict access to data, secure systems and networks, and respond to security incidents.[2]

In May 2006, VA initially announced that computer equipment containing personally identifiable information on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA

[1] Information security controls include access controls, configuration management, segregation of duties, and contingency planning. These controls are designed to ensure that access to data is appropriately restricted, only authorized changes to computer programs are made, computer security duties are segregated, and backup and recovery plans are adequate to ensure the continuity of essential operations.

[2] We made recommendations to address weaknesses in June 2002 as part of our review of VA's security management program to ensure compliance with Government Information Security Reform legislation. In December 2002, Congress enacted the Federal Information Security Management Act, which required each agency to use a risk based approach to develop, document, and implement a departmentwide information security program. Since our report in 2002, the IG has continued to make recommendations to address weaknesses in the department's information security program as part of its annual review of the program under the act.

employee.[3] Until the equipment was recovered, veterans did not know whether their information was likely to be misused. The security incident highlighted the vulnerability of sensitive information on VA's systems to inadvertent or deliberate misuse, loss, or improper disclosure.

This report responds to your request for a review of the department's actions to improve information security. Specifically, our objectives were to evaluate (1) whether VA has effectively addressed GAO and VA IG recommendations and (2) actions VA has taken since the May 2006 security incident to strengthen its information security practices and secure personal information.

In addressing our objectives, we examined and analyzed agency policies, procedures, plans, and artifacts; interviewed key agency and IG personnel; and assessed the effectiveness of implemented actions. We also performed audit procedures to determine the extent to which VA has installed encryption functionality on laptop computers at eight locations. We performed our work at VA headquarters in Washington, D.C., and at select VA facilities, from November 2006 through August 2007, in accordance with generally accepted government auditing standards. For more details on our objectives, scope, and methodology, see appendix I.

Results in Brief

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. VA has implemented two GAO recommendations: to develop a process for managing its action plan to correct identified weaknesses and to regularly report to the Secretary on progress in updating its security plan. 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 when appraising the department's senior executives. In addition, the department has not yet fully implemented 20 of 22 information security-related recommendations made by the IG in 2006. For example, VA has not completed critical management activities to appropriately restrict access to data, networks, and department facilities;

[3] "Personally identifiable information" refers to any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc., or any other personal information that is linked or linkable to an individual.

ensure that only authorized changes and updates to computer programs are made; and strengthen critical infrastructure planning to ensure information security requirements are addressed. Because these recommendations have not yet been implemented, unnecessary risk exists that personal information of veterans and other individuals, such as medical providers, will be exposed to data tampering, fraud, and inappropriate disclosure.

Since the May 2006 security incident, VA has begun or continued several major initiatives to strengthen information security practices and secure personal information within the department, but more remains to be done. These initiatives include continuing the department's efforts, begun in October 2005, to reorganize its management structure to provide better oversight and fiscal discipline over its IT systems; developing a remedial action plan; establishing an information protection program; improving its incident management capability; and establishing an office responsible for oversight and compliance of IT within the department. However, although these initiatives have led to progress, their implementation has shortcomings. For example,

- responsibility for managing and implementing the VA security program (an essential element for ensuring compliance with the Federal Information Security Management Act) is split between separate offices, and no documented process exists for the responsible officials to coordinate with each other;

- the position of the chief information security officer has been unfilled since June 2006;

- although numerous action items in the department's remedial action plan are tasks to develop, document, revise, or update a policy or program, 87 percent of these have no corresponding task with an established time frame for implementation across the department;

- VA does not have clear guidance for identifying devices that require encryption functionality;

- procedures for incident response and notification do not include mechanisms for consultation with outside agencies on mitigation options; and

- the departmental 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.

As a result of such weaknesses, the effectiveness of VA initiatives to strengthen information security practices at the department may be limited.

We are making 17 recommendations to the Secretary of Veterans Affairs aimed at helping the department to improve the effectiveness of VA's efforts to strengthen information security practices, including developing and documenting processes, policies, and procedures; fill a key position; and completing the implementation of key initiatives.

In providing written comments on a draft of this report (which are reprinted in appendix IV), the Deputy Secretary of Veterans Affairs generally agreed with our findings and recommendations. The Deputy Secretary stated that VA has already implemented or is working to implement all 17 recommendations.

Background

With over 235,000 employees, including physicians, nurses, counselors, statisticians, computer specialists, architects, and attorneys, VA is the second largest federal department. It carries out its mission through three agency organizations—Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration—and field facilities throughout the United States. The department provides services and benefits through a nationwide network of 156 hospitals, 877 outpatient clinics, 136 nursing homes, 43 residential rehabilitation treatment programs, 207 readjustment counseling centers, 57 veterans' benefits regional offices, and 122 national cemeteries. In carrying out its mission, the department depends on IT and telecommunications systems, which process and store sensitive information, including personal information on veterans.

Information security is a critical consideration for any organization that depends on information systems and networks to carry out its mission or business. It is especially important for government agencies, where maintaining the public's trust is essential. The dramatic expansion in computer interconnectivity and the expanding use of mobile devices and storage media are changing the way our government, the nation, and much of the world share information and conduct business. Without proper safeguards, enormous risk exists that systems, mobile devices, and information are exposed to potential 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 December 2002,[4] which permanently authorized and strengthened the information security program, evaluation, and reporting requirements established by earlier legislation (commonly known as GISRA, the Government Information Security Reform Act).[5] FISMA sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. The act requires each agency to develop, document, and implement an agencywide information security program for the data and systems that support the operations and assets of the agency, using a risk-based approach to information security management. According to FISMA, the head of each agency has responsibility for delegating to the agency chief information officer (CIO) the authority to ensure compliance with the security requirements in the act. To carry out the CIO's responsibilities in the area, a senior agency official is to be designated chief information security officer (CISO).

Prior GAO and IG Work Related to VA Information Security

In June 2002, we reported that VA had not completed actions to strengthen its security management program, ensure compliance with security policies and procedures, and ensure accountability for information security throughout the department.[6] We made four recommendations to VA: (1) complete a comprehensive security management program that included actions related to central security management functions, risk assessments, security policies and procedures, security awareness, and monitoring and evaluating computer controls; (2) develop a process for managing the department's updated security plan to remediate identified weaknesses; (3) regularly report to the Secretary, or his designee, on progress in implementing VA's security plan; and (4) ensure consistent use

[4] FISMA, Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

[5] GISRA was enacted as subtitle G of Title X of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, Pub. L. No. 106-398 (Oct. 30, 2000). GISRA was to expire 2 years after its effective date.

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

of information security performance standards when appraising the department's senior executives.

Since our report in 2002, VA's IG has made additional recommendations addressing serious weaknesses within the department's information security controls. In March 2005, the VA IG reported that the department had not appropriately restricted access to data, ensured that only authorized changes were made to computer programs, ensured that backup and recovery plans were adequate to ensure the continuity of essential operations, and moved the VA Central Office data center to a more appropriate location.[7] The IG made a number of recommendations to the department to secure patient information and data over VA networks, improve application and operating system change controls, test continuity of operations plans at national data centers, and complete the move of the VA Central Office data center. In its annual FISMA report for fiscal year 2005, issued in September 2006, the IG carried forward all the recommendations from its prior years' FISMA audits. It made recommendations in 17 areas to address all FISMA related findings for the fiscal year.[8]

Significant Security Incidents Reported

On May 3, 2006, the home of a VA employee was burglarized, resulting in the theft of a personally owned laptop computer and external hard drive that contained personal information on approximately 26.5 million veterans and U.S. military personnel. The external hard drive was not encrypted or password protected.[9] The Secretary of VA was notified of the theft on May 16, 2006, and Congress and veterans were notified on May 22, 2006. Notification letters were sent to all veterans, and VA announced that free credit monitoring services would be offered.

A number of congressional hearings were held and bills introduced related to the protection of veterans' privacy and identity. During this time period,

[7] Department of Veterans Affairs Office of Inspector General, *Audit of the Department of Veterans Affairs Information Security Program*, Report No. 04-00772-122 (Washington, D.C.: Mar. 31, 2005).

[8] Department of Veterans Affairs Office of Inspector General, *FY2005 Audit of VA Information Security Program*, Report No. 05-00055-216 (Washington, D.C.: Sept. 20, 2006).

[9] Encryption is used to provide basic data confidentiality and integrity for data, by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm.

many veteran service organizations expressed concerns to Congress as to whether VA was capable of safeguarding the personal information of veterans. These organizations also expressed doubt over whether the department's attempts to correct the weaknesses would be effective.

The stolen computer equipment was recovered on June 28, 2006, and forensic testing by the Federal Bureau of Investigation determined that the sensitive data files had not been accessed or compromised. After the equipment was recovered, the Office of Management and Budget (OMB) withdrew its request to Congress for funding for the free credit monitoring services because it had concluded that credit monitoring services were no longer necessary due to the results of the FBI's analysis. Veterans' organizations indicated that the department should continue to offer credit monitoring services in order to allay veterans' worries regarding the potential of identity theft. As a result of the theft, the VA IG issued a report in July 2006 on the investigation of the incident and made five recommendations to improve VA's policies and procedures for securing sensitive information and conducting security awareness training.[10]

Recognizing the concerns of veterans, in December 2006, Congress passed the Veterans Benefits, Health Care, and Information Technology Act of 2006.[11] Under the act, the VA's CIO is responsible for establishing, maintaining, and monitoring departmentwide information security policies, procedures, control techniques, training, and inspection requirements as elements of the departmental information security program. The act also includes provisions to further protect veterans and service members from the misuse of their sensitive personal information. In the event of a security incident involving personal information, VA is required to conduct a risk analysis, and on the basis of the potential for compromise of personal information, the department may provide security incident notifications, fraud alerts, credit monitoring services, and identity theft insurance. Congress is to be informed regarding security incidents involving the loss of personal information.

[10] Department of Veterans Affairs Office of Inspector General, *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans*, Report No. 06-02238-163 (Washington, D.C.: July 11, 2006).

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

On January 22, 2007, a security incident at a research facility in Birmingham, Alabama, highlighted other potential risks associated with the loss of information. The incident involved the loss of information on 1.3 million medical providers from the Centers for Medicare & Medicaid Services of the Department of Health and Human Services, as well as information on 535,000 individuals. [12] In its report on the Birmingham incident, the VA IG noted that the information compromised in the incident could potentially be used to compromise the identity of physicians and other health care providers and commit Medicare billing fraud.[13] VA took action to respond to the loss of provider information by requesting the Department of Health and Human Services to conduct an independent risk analysis on the provider data loss. The risk analysis concluded that there was a high risk that the loss of personal information could result in harm to the individuals concerned, and the Centers for Medicare & Medicaid Services sent a letter to VA on March 28, 2007, requesting that credit monitoring services be offered to providers. The department mailed notification letters to providers starting on April 17, 2007, and offered credit monitoring services. In addition, the Centers for Medicare & Medicaid Services indicated that VA might need to take additional measures to mitigate any risk of further harm, but it did not specify what such action might be or specifically mention Medicare fraud.

VA Has Not Fully Implemented GAO and IG Recommendations

Although VA has made progress, it has not yet fully or effectively implemented two of four GAO recommendations and has not fully implemented 20 of 22 IG recommendations to strengthen its information security practices. Because these recommendations have not yet been implemented, unnecessary risk exists that personal information of veterans and others would be exposed to data tampering, fraud, and inappropriate disclosure.

VA Has Not Implemented Two of Four GAO Recommendations

VA has implemented two of our recommendations. However, it has not fully implemented two other GAO recommendations. In response to our recommendation that it regularly report on progress in updating its

[12] This included, among other things, the unique physician identification number, Medicare billing number, and physician credential code of medical providers.

[13] Department of Veterans Affairs Office of Inspector General, *Administrative Investigation Loss of VA Information VA Medical Center Birmingham, AL*, Report No. 07-01083-157 (Washington, D.C.: June 29, 2007).

security plan to the Secretary, the department CIO took immediate steps in 2002 to begin briefing the Secretary and Deputy Secretary on a regular basis. Regarding our recommendation that it develop a process for managing its remedial action plan, VA issued, in May 2006, its IT Directive 06-1, which established the Data Security-Assessment and Strengthening of Controls Program to remedy weaknesses in managing its action plan. It also hired a contractor to develop Web-based tools to assist department officials in managing and updating the plan on a biweekly basis.

However, it has not fully implemented our remaining two recommendations. First, although it has taken action, VA has not yet fully implemented our recommendation to complete a comprehensive security management program, including actions related to central management functions, security policies and procedures, risk assessments, security awareness, and monitoring and evaluating computer controls. In August 2006, VA issued Directive 6500, which documented a framework for the department's security management program and set forth roles and responsibilities for the Secretary, CIO, and CISO to ensure compliance with FISMA requirements. VA also developed, documented, and implemented security policies and procedures for certain central management functions and security awareness training. In addition, it implemented a process for tracking the status of security weaknesses and analyzing the results of computer security reviews using software tools the department had developed.

As part of implementing the department's security directive (Directive 6500), VA planned to issue Handbook 6500 to provide guidance for developing, documenting, and implementing the elements of the information security program. However, it has not finalized and approved this handbook, which has been in draft form since March 2005. The handbook contains the VA National Rules of Behavior,[14] as well as key guidance for minimum mandatory security controls, performing risk assessments, updating security plans, and planning for continuity of operations. This guidance is to be used as VA undertakes these activities as part of its preparation for completing the recertification and re-accreditation of its systems by August 2008 and to comply with provisions of the Veterans Benefits, Health Care, and Information Technology Act of

[14] The VA National Rules of Behavior is a set of department rules that describes the responsibilities and behavior of personnel with regard to information system usage and is required to be developed under the Veterans Benefits, Health Care, and Information Technology Act of 2006.

2006. VA officials indicated the handbook was close to completion, but they did not provide an estimated time frame for completion. Until the handbook is finalized and approved, VA cannot be assured that department staff are consistently coordinating security functions that are critical to safeguarding its assets and sensitive information against potential data tampering, disruptions in critical operations, fraud, and the inappropriate disclosure of sensitive information.

Second, VA has not fully implemented our recommendation to ensure consistent use of information security performance standards in appraising the department's senior executives. In September 2006, VA issued a memorandum that required all senior executive performance plans, which include performance elements and expectations, to include information security as an evaluation element by November 30, 2006. According to VA, senior executive performance plans were reviewed by human resource officials, and the plans complied with the memorandum. However, VA was unable to provide documentation on the performance plan reviews or a documented process for regular review of the plans.[15] As a result, it is unknown whether the department can appropriately hold management accountable for information security. Until VA develops, documents, and implements a process for reviewing the senior executive performance plans on a regular basis to ensure that information security is included as an evaluation element, it may not have the appropriate management accountability for information security.

VA Has Not Fully Implemented IG Recommendations

Although VA has implemented 2 recommendations made by the IG, it has not yet fully implemented 20 other IG recommendations. For example, in response to the IG's recommendation that the department complete actions to relocate and consolidate the Central Office's data center, it moved servers and network hardware to other VA locations. Regarding the recommendation to research the benefits and costs of deploying intrusion prevention systems at all sites, the department began installing intrusion prevention systems at all sites. However, the department has not completed critical management activities to implement 15 of the 17 recommendations made by the IG in September 2006, which were carried forward from its March 2005 report, to appropriately restrict access to

[15] Such a review process and documentation of it are control activities identified in GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

data, networks, and VA facilities; ensure that only authorized changes and updates to computer programs are made; strengthen critical infrastructure planning to ensure information security requirements are addressed; and ensure that background investigations are conducted on all applicable employees and contractors. To begin addressing these recommendations, VA has drafted policies and procedures, implemented certain technical solutions, and relocated data center servers to new locations at VA facilities. However, according to the department's action plan to remediate weaknesses, all actions to resolve IG recommendations will not be completed until 2009. A detailed description of the actions VA has taken or plans to take to address the IG's 17 recommendations can be found in appendix II.

VA has also made some progress in addressing the five recommendations from the IG's July 2006 report on the investigation of the May laptop theft incident. However, it has not fully implemented corrective actions. To begin addressing these recommendations, VA has drafted policies and procedures and updated its Cyber Security Awareness training course. However, VA is still in the process of finalizing standard contracting language to ensure that contractor personnel are held to the same standards as department personnel; it is also still standardizing all IT position descriptions and ensuring that they are evaluated, have proper sensitivity level descriptions, and are consistent throughout the department. Until these actions are complete, VA has limited assurance that it has the proper safeguards in place to adequately protect its sensitive information from inadvertent or deliberate misuse, loss, or improper disclosure.

By Not Fully Implementing GAO and IG Recommendations, VA Leaves Personal Information Vulnerable

The need to fully implement GAO and IG recommendations to strengthen information security practices is underscored by the prevalence of security incidents involving the unauthorized disclosure, misuse, or loss of personal information of veterans and other individuals, such as medical providers. Between December 2003 and April 2006, VA had at least 700 reported security incidents involving the loss of personal information. For example, one incident in 2003 involved the theft of a laptop containing personal information on 100 veterans from the home of a VA employee. In 2004, personal computers that contained data on 2,000 patients were stolen from a locked office in a research facility. In 2005, information on 897 providers was inappropriately disclosed over VA's e-mail system. In addition, in 2006, employee medical records were inappropriately accessed by a VA staff member, and a hacker compromised a computer system at a medical center supporting 79,000 veterans. All these incidents were partially attributable to weaknesses in internal controls.

More recently, additional incidents have occurred that, like the earlier incidents, were partially due to weaknesses in the department's security controls. In these incidents, which include the May 2006 theft of computer equipment from an employee's home (discussed earlier) and the theft of equipment from department facilities, millions of people had their personal information compromised. Appendix III provides details on a selection of incidents that occurred between December 2003 and January 2007.

Although VA has made some progress in implementing GAO and IG recommendations to resolve these weaknesses in security controls, all actions to resolve these recommendations are not planned to be implemented until 2009. As a result, VA will be at increased risk that systems, mobile devices, and information may be exposed to potential data tampering, disruptions in critical operations, fraud, and the inappropriate disclosure of sensitive information.

VA Is Undertaking Several Major Initiatives to Strengthen Information Security, but Implementation Has Shortcomings

VA has begun or continued several major initiatives since the May 2006 security incident to strengthen information security practices and secure personal information within the department, but more remains to be done. Since October 2005, VA has been reorganizing its management structure to provide better oversight and fiscal discipline over its IT systems, and it has undertaken a series of new initiatives. However, shortcomings with the implementation of these initiatives limit their effectiveness. For example, although VA has developed a remedial action plan that includes tasks to develop, document, revise, or update a policy or program, 87 percent of these do not have an established time frame for implementation across the department. Unless such shortcomings are addressed, these initiatives may not effectively strengthen information security practices at the department.

Realignment of IT Management Structure

An effective IT management structure is the starting point for coordinating and communicating the continuous cycle of information security activities necessary to address current risks on an ongoing basis while providing guidance and oversight for the security of the entity as a whole. Under FISMA and the Veterans Benefits, Health Care, and Information Technology Act of 2006, the CIO ensures compliance with requirements of these laws and designates a senior agency information security officer or

CISO to assist in carrying out his responsibilities. One mechanism organizations can adopt to achieve effective coordination and communication is to establish a central security management office or group to coordinate departmentwide security-related activities.[16] To ensure that information security activities are effective across an organization, an IT management structure should also include clearly defined roles and responsibilities for all security staff and coordination of responsibilities among individual staff.

The department officially began its effort to provide the CIO with greater authority over IT in October 2005 by realigning its management organization to a centralized management structure. By July 2006, a department contractor began work to assist with the realignment effort. According to VA, its goals in moving to a centralized management structure were to provide the department better oversight over the standardization, compatibility, and interoperability of IT systems, as well as better overall fiscal discipline. The Secretary approved the department's new IT organization structure in February 2007. The new structure includes an Assistant Secretary for Information and Technology (who serves as VA's CIO), the CIO's Principal Deputy Assistant Secretary, and five Deputy Assistant Secretaries. Five new senior leadership positions within the Office of Information and Technology were created to assist the CIO in overseeing five core IT process areas: cyber security, portfolio management, resource management, systems development, and operations. Completion of the realignment is scheduled for July 2008.[17]

Under the new IT management structure, responsibility for information security functions within the department is divided between two core process areas:

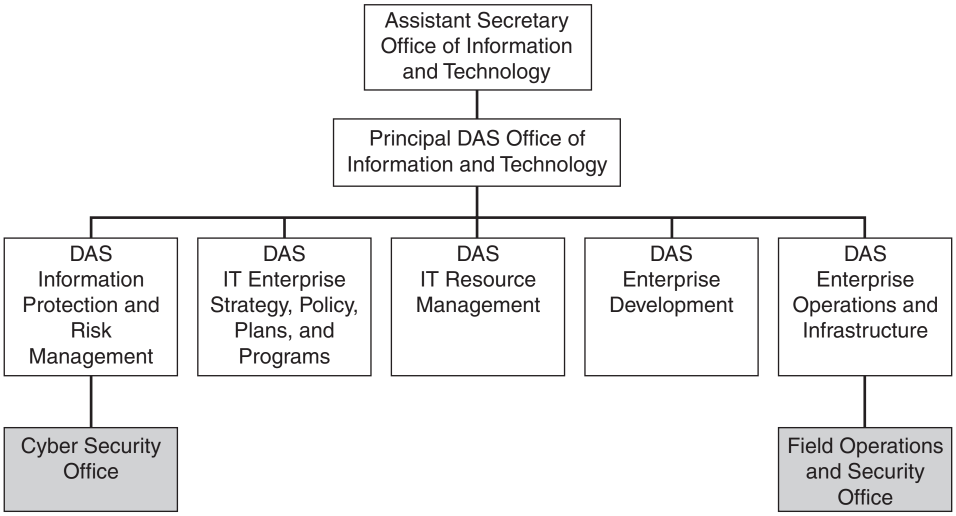
[16] This is one of the identified activities described in our 1998 study of security management practices: GAO, *Executive Guide: Information Security Management—Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[17] We recently recommended that VA improve its management of the realignment effort by dedicating an implementation team to manage change, expediting development of performance metrics, and establishing a schedule for implementing management processes. VA agreed with the findings in our report and generally concurred with the recommendations. GAO, *Veterans Affairs: Continued Focus on Critical Success Factors Is Essential to Achieving Information Technology Realignment*, GAO-07-844 (Washington, D.C.: June 15, 2007).

- First, the Director of the Cyber Security Office (part of the Information Protection and Risk Management process area) has responsibility for developing and maintaining a departmentwide security program; overseeing and coordinating security efforts across the organization; and managing the development and implementation of department security policy, standards, guidelines, and procedures to ensure ongoing maintenance of security. The Director of Cyber Security is also the designated CISO for the department.
- Second, the Director of the Field Operations and Security Office (part of the Enterprise Operations and Infrastructure process area) is responsible for implementing security and privacy policies, validating compliance with certification and accreditation requirements, and managing facility information security officers.

In brief, the CISO/Director of Cyber Security is thus responsible for managing the departmentwide security program, but the Director of the Field Operations and Security is responsible for implementing it. Figure 1 shows these two offices within the new management structure.

Figure 1: Office of Information and Technology Organization Chart


Assistant Secretary Office of Information and Technology
Principal DAS Office of Information and Technology
DAS Information Protection and Risk Management
DAS IT Enterprise Strategy, Policy, Plans, and Programs
DAS IT Resource Management
DAS Enterprise Development
DAS Enterprise Operations and Infrastructure
Cyber Security Office
Field Operations and Security Office

Source: VA.

Note: DAS = Deputy Assistant Secretary.

Although VA has made significant progress in the realignment of its IT management structure, no documented process yet exists for the two responsible offices to coordinate with each other in managing and implementing a departmentwide security program. VA officials indicated that the Director of Cyber Security and the Director of Field Operations and Security are communicating about the implementation of security policies and procedures within the department. However, this communication is not defined as a role or responsibility for either position in the new management organization book, nor is there a documented process in place to coordinate the management and implementation of the security program, both of which are key security management practices. As a result, policies or procedures could be inconsistently implemented throughout the department. Without a consistently implemented departmentwide security program, the CISO cannot effectively ensure departmentwide compliance with FISMA. Until the process and responsibilities for coordinating the management and implementation of IT security policies and procedures throughout the department are clearly documented, VA will have limited assurance that the management and implementation of security policies and procedures are effectively coordinated and communicated.

In addition, the CISO position is currently unfilled, hindering VA's ability to strengthen information security practices and coordinate security-related activities within the department. The CISO position has been vacant since June 2006, and currently, the CIO is the acting CISO of the department. The department has been attempting to fill the position of the CISO since October 2006. In addition, the department began trying to hire staff for other senior positions in March 2007. VA officials have indicated that the process and procedures they are required to undertake to hire staff for the positions is quite extensive and takes time to complete. Nevertheless, until the position of the CISO is filled, the department's ability to strengthen information security will continue to be hindered.

Furthermore, the department's directive on its information security program has not been updated to reflect the new IT realignment structure for the position of the CISO. Under Directive 6500, the Associate Deputy Assistant Secretary for Cyber and Information Security is the senior information security officer or CISO. However, under the new realignment structure, there is no Associate Deputy Assistant Secretary for Cyber and Information Security, and instead the Director of Cyber Security is the CISO. VA officials have said that they intend to revise the directive to reflect the new management structure, but they did not provide an estimated time frame for completion. If roles and responsibilities are not updated or consistent in VA's policies and directives, then communication and coordination of responsibilities among the department's security staff may not be sufficient.

Development of Action Plan to Remediate Identified Weaknesses

Action plans to remediate identified weaknesses help departments to identify, assess, prioritize, and monitor progress in correcting security weaknesses that are found in information systems. According to OMB's revised Circular A-123, *Management's Responsibility for Internal Control*, departments should take timely and effective action to correct deficiencies that they have identified through a variety of information sources. To accomplish this, remedial action plans should be developed for each deficiency, and progress should be tracked for each.

Following the May 2006 security incident, VA officials began working on an action plan to strengthen information security controls at the department. Referred to as the Data Security-Assessment and Strengthening of Controls Program, the plan was developed over a period of several months, and work has been completed on some tasks. By the end of January 2007, 20 percent of the items in the action plan had been completed, and task owners had been assigned for all items in the plan. As of June 1, 2007, the plan had at least 400 items to improve security and address weaknesses that the IG has identified at the department.

On a biweekly basis, the action plan is updated with status updates provided by the task owners (including the percentage of work completed to resolve the item), and a new version of the plan is created. The CIO receives a briefing on each new version of the action plan. Once the new version is approved by the CIO, the plan is made available to task owners and other officials at the department. The CIO has also briefed other senior department officials on the plan and action items.

Although VA's action plan has task owners assigned and is updated biweekly, department officials have not ensured that adequate progress has been made to resolve items in the plan. First, in more than a third of cases, VA has not completed action items by their expected completion date. Specifically, VA has extended the completion date at least once for 38 percent of the plan items, and it has extended the completion date multiple times for 6 percent of the items in the plan. The average extension was about 5 months. In addition, 28 percent of action items that remained open as of June 1, 2007, had already exceeded the scheduled completion date, and over half of the work remained to be completed for a majority of those items. These extensions and missed deadlines can be attributed in part to VA's not developing, documenting, and implementing procedures to ensure that action items were addressed in an effective and timely manner. If weaknesses are not successfully corrected in a timely manner, VA will continue to lack effective security controls to safeguard its assets and sensitive information.

Second, a large portion of VA's approach to correcting identified weaknesses has been focused on establishing policies and procedures: 39 percent of the items in the action plan are to develop and document or revise and update a policy, a program, or criteria. However, VA has not established action items for implementing these new or changed policies and procedures across the department. For 87 percent of action items related to policies and procedures, the action plan included no corresponding task with an established time frame for departmentwide implementation. Developing and documenting policies and procedures are just the first two steps in remediating identified weaknesses. If there are no implementation tasks with time frames, VA cannot monitor and ensure successful implementation. Until VA establishes tasks with time frames to implement policies and procedures in the plan, it will not be able to successfully manage its planned actions to correct identified weaknesses.

Third, VA does not have a process in place to validate the closure of action plan items, that is, to ensure both that task owners have completed the activities required to sufficiently address action items and also that there is adequate documentation of these activities. During our review, we noted the closure of approximately 80 action items that included activities such as developing a policy or procedure, creating a schedule, deploying security tools, or updating software. However, according to the department official responsible for managing the plan, upon review of these completed items, VA found a number of them lacked support for closing the item (such as documentation). This official indicated that VA was developing a process to provide validation of closed action plan items, but no supporting documentation on the development of this validation process had been provided. Until VA develops, documents, and implements a process to validate the closure of action plan items, it will not be assured that closed action items have been sufficiently addressed.

Fourth, VA's action plan does not identify the activities it is taking to address our recommendations. In November 2006, the VA official in charge of managing the plan indicated that although the department had not previously identified activities being taken to address our recommendations, it would begin to do so. However, as of June 2007, these activities had not been identified and tracked in the action plan. As a result, VA may not be able to adequately monitor its progress in implementing our recommendations to resolve identified weaknesses. Until VA identifies the activities it is taking in its action plan to address our recommendations, it will have limited assurance that progress in implementing those activities is being adequately monitored.

Establishment of Information Protection Program

VA has developed its Information Protection Program, which is a phased approach to ensuring that the department has the appropriate software tools to assist in ensuring the confidentiality, availability, and integrity of information. During the first phase, VA installed encryption software on laptops across the department, a task completed in September 2006. In the second phase, the department is undertaking several other information protection initiatives, including improving the security of network transmissions and the protection of removable storage devices, such as the encryption of thumb drives. These initiatives are all currently being developed and documented.

Encryption of VA Laptops

One mechanism to enforce the confidentiality and integrity of critical and sensitive information is the use of encryption. Encryption transforms plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. According to VA Directive 6504, issued in June 2006, approved encryption software must be installed if an employee uses VA government-furnished equipment or other non-VA equipment in a mobile environment, such as a laptop or PDA carried out of a department office or a personal computer in an alternative worksite, and the equipment stores personal information. The encryption software used must meet Federal Information Processing Standard 140.[18]

According to department officials, by September 2006, the department had successfully encrypted over 18,000 laptops. The laptops were encrypted through a combination of two software encryption products, both of which have been certified as complying with the provisions of Federal Information Processing Standard 140. Simultaneously, VA developed and implemented routine laptop "health checks." These checks ensure that all laptops have applied updated security policies, such as antivirus software, and will also remove any sensitive information that is not authorized to be stored on the laptop.

Based on the results of our testing, VA consistently implemented encryption software at eight VA facilities, with minor exceptions.[19] At six

[18] Federal Information Processing Standard 140 is published by National Institute of Standards and Technology and provides a standard that specifies the security requirements that will be satisfied by a cryptographic module used by federal agencies.

[19] See appendix I for more details regarding our methodology for testing the implementation of encryption on laptops. Because of the scope of our testing of laptop encryption, we could not make a determination of the effectiveness of VA's effort to implement VA Directive 6504 at all department facilities.

of the eight facilities, all laptops were encrypted in accordance with the directive. At the other two facilities, both medical centers, the directive was not implemented in a small number of cases. At one medical center, of the 58 laptops tested, 3 should have been encrypted according to VA's policy but were not. At another medical center, of the 41 laptops tested, 1 laptop was not encrypted that should have been. In some of these cases, VHA medical center officials noted that the reference in the directive to operation in a mobile environment led to ambiguity about which laptops were required to be encrypted.[20]

Although our testing showed sound consistency in this encryption effort, this and another source of ambiguity in the directive could affect the department's success in implementing other planned encryption initiatives. Specifically, Directive 6504 did not provide explicit guidance on whether to encrypt laptops that were categorized as medical devices, which make up a significant portion of the population of laptops at VHA facilities.[21] At facilities for patient care, laptops could be categorized both as equipment that operated in a mobile environment (and thus subject to VA's encryption directive) and as medical devices (and thus subject to compliance with other federal guidance that may interfere with following the encryption directive).[22] At the two medical centers we visited, which each have over 300 laptops, most laptops were considered medical devices. When VHA officials contacted the help desk for the encryption initiative, they were told that these laptops did not need encryption software installed. However, Directive 6504 had not made this clear, increasing the challenge to VHA facilities in implementing the encryption initiative. Without guidance that takes into consideration the environment in which laptops are used in different VA facilities and that clearly identifies devices that require encryption functionality, VA may not have assurance that all facilities in the department will be able to consistently implement encryption initiatives for all appropriate devices.

[20] In contrast, VBA directed that all laptops at each facility be encrypted regardless of whether or not they operated in a mobile environment.

[21] VA has since hired a contractor to analyze the relationship between the biomedical and IT functions in the devices to improve the management of medical devices.

[22] The Food and Drug Administration's guidance provides that medical device software (that is, software that is used as a component or accessory of a medical device) must be validated by the manufacturer before it can be used. When any change to the software is made, the change must be validated; this requirement limits VA's ability to encrypt laptops that are considered medical devices.

Finally, the department did not maintain an accurate inventory of all laptops that had been encrypted, nor did it have an inventory of all laptops within the department. Each VA facility was responsible for maintaining an inventory of laptops, including what laptops had been encrypted, but the laptop inventories at four of the eight facilities we visited were inaccurate. For example, eight laptops listed in the inventories were not laptops, but scanners, personal computers or other devices. In some cases, the inventory listed a laptop as encrypted, but testing revealed that the machine was not encrypted. (The weaknesses identified with the inventories of laptops are similar to weaknesses identified in a report we recently issued, which noted significant IT inventory control weaknesses at VA).[23] Because it did not maintain an accurate inventory of all equipment that has encryption installed, VA may not have adequate assurance that all equipment required to be encrypted has been.

Development of Additional Information Protection Initiatives

As part of its phased approach to acquiring appropriate software tools, the department is undertaking several information protection initiatives. For instance, the department is working to secure network transmissions to prevent user identification, passwords, and data from being transmitted in clear text. To provide port security and device control, VA is establishing access permission lists, audit and reporting capabilities, and lists of approved devices. For the protection of removable storage media, VA developed and documented Directive 6601, which provides guidance for use of removable devices, and it is in the process of acquiring encryption software for thumb drives, external hard drives, and CD-ROM and DVD drives. VA is also acquiring encryption for mobile devices such as Blackberries. In addition, the department is establishing a public key infrastructure and Internet gateway for secure e-mail transmission and document exchange. These initiatives are in varying stages of development and have not yet been implemented.

Improvement of Incident Management Capability

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they take prompt steps to detect and respond to them before significant damage can

[23] GAO, *Veterans Affairs: Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation*, GAO-07-505 (Washington, D.C.: July 16, 2007), and *Veterans Affairs: Lack of Accountability and Control Weaknesses over IT Equipment at Selected VA Locations*, GAO-07-1100T (Washington, D.C.: July 24, 2007).

be done. In addition, analyses of security incidents can pinpoint vulnerabilities that need to be eliminated, provide valuable input for risk assessments, help in prioritizing security improvement efforts, and be used to illustrate risks and related trends for senior management. FISMA requires that agencies develop procedures for detecting, reporting, and responding to security incidents. In addition, OMB Memo M-06-19 requires agencies to report all incidents involving personal identifiable information to the U.S. Computer Emergency Readiness Team (US-CERT) within 1 hour of discovering the incident.[24]

Incident Detection, Reporting, and Response

VA has improved its incident management capability since May 2006 by realigning and consolidating two centers with responsibilities for incident management, as well as developing and documenting key policies and procedures. Following the May 2006 security incident, VA hired a contractor to assist its Network Operations Center and Security Operations Center in developing plans for improved coordination between the two centers and for using a risk management approach to managing incidents. As part of its findings, the contractor recommended that the two centers be integrated at the regional and enterprise level. In February 2007, VA realigned and consolidated the two centers into the Network and Security Operations Center (NSOC), which is responsible for incident detection or identification, response, and reporting within the department. NSOC has also developed and documented a concept of operations for incident management and call center procedures, and it has developed a new incident report template to assist VA personnel in reporting incidents to the center within 1 hour of discovering the incident. Senior management officials also receive regular reports on security incidents within the department.

In addition, VA has improved the reporting of incidents involving the loss of personal information within the department since the May 2006 incident. Following the incident, the Secretary issued a memorandum requiring all employees to take security and privacy training by June 30, 2006, as well as sign a statement of commitment and understanding regarding the handling of personal information of veterans. An analysis of reported incidents from 2003 to 2006 showed a significant increase in the reporting of incidents involving the loss of personal information to NSOC

[24] OMB Memorandum M-06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments” (July 12, 2006).

in 2006, as detailed in table 1. Of the incidents reported in 2006, 77 percent were reported after May.

Table 1: Number of Incidents by Type Reported to NSOC from January 2003 to November 2006

Type of incident involving the loss of personal information	2003	2004	2005	2006[a]
Records lost or misplaced	19	58	41	316
Records or hardware stolen	7	9	14	65
Improper disposal of records	10	27	10	80
Unauthorized access	60	120	112	255
Unencrypted e-mails sent	8	13	16	170
Unintended disclosure or release	22	48	24	199
Total number of incidents	**126**	**275**	**217**	**1085**

Source: GAO analysis of VA data on incidents.

[a]Numbers reported are from January 1, 2006, to November 3, 2006.

While the increase in reported incidents shows that the memorandum and updated security and privacy training are heightening VA employees' awareness of their responsibility to report incidents involving loss of personal information, it also indicates that vulnerabilities remain in security controls designed to adequately safeguard information. To assist the department in improving its analysis of security incident data, NSOC merged three incident databases into one to streamline the collection of incident data gathered within the department. VA also developed a software tool with a Web-based interface (the Formal Event Review and Evaluation Tool) to analyze reported incidents and observe trends, and began using the tool in April 2007.

Incident Notification

The department has made a notable improvement in its notification of major security incidents to US-CERT, the Secretary, and Congress since the incidents in May 2006.[25] However, the time it took to send notification letters to individuals was increased for some incidents because VA did not have adequate procedures for incident response and notification. Table 2 presents major security incidents occurring since May 2006, along with the times taken to make various notifications. As the table shows, delays in reporting incidents have generally decreased since May 2006.

[25] For more details on these incidents at VA, see appendix III.

Table 2: Time Elapsed Between Major Incidents at VA and Notification of US-CERT, Secretary, Congress, and Individuals (May 2006 to January 2007).

		Time taken to report or send notification letter (in calendar days)			
Security incident	Incident date	To US-CERT	To VA Secretary	To Congress	To individuals
Computer equipment stolen from VA employee home	May 3, 2006	20 days	13 days	19 days	About a month[a]
Backup tape missing	May 5, 2006	42 days	18 days	55 days	159 days
Desktop computer stolen from contractor facility	August 3, 2006	Same day	1 day	1 day	7 days
Medical device in New York stolen	September 6, 2006	Same day	Same day	Within a week	55 days
External hard drive stolen at Birmingham facility	January 22, 2007	Same day	1 day	11 days	49 days (individuals); 85 days (medical providers)

Source: GAO analysis of VA data.

[a] Because of the volume of letters that were sent out, notification letters were sent out over a period of time during the month of June 2006.

Coordination with other agencies. In the incident in Birmingham in January 2007, medical provider and physician information from the Centers for Medicare & Medicaid Services of the Department of Health and Human Services was lost, requiring VA to coordinate with this department to respond to the incident. At the time of the incident, VA had drafted interim procedures for incident response, including notifying individuals affected by security incidents.[26] These draft procedures described steps to be taken to respond to incidents involving the loss of information on veterans. However, they did not include processes for coordinating incident response and mitigation activities with other agencies. This contributed to the fact that it took more time to determine

[26] VA drafted these interim procedures to comply with the Veterans Benefits, Health Care, and Information Technology Act of 2006, which required VA to draft regulations for security incident notification and publish these in the *Federal Register* for public comment for 60 days. Until the regulation could be finalized, VA followed its interim procedures.

the risks to medical providers, who were not notified until 85 days after the incident.

To address the coordination issue, VA revised its interim procedures to indicate that incident response teams will work with other federal agencies and teams as needed to contract for independent analyses of the risk associated with compromise of the particular data involved. In March 2007, VA approved these revised interim procedures. However, the approved procedures are limited to contracting for risk analyses and do not incorporate processes for coordinating with other federal agencies on other appropriate mitigation activities. For example, although the procedures allow for the offer of credit monitoring to affected individuals, they do not address mitigating other types of risks, such as potential fraudulent claims for payment under Medicare, which were a potential risk for the Birmingham incident. Credit monitoring would not address this risk. Other coordination and mitigation activities may be needed, such as alerting the Centers for Medicare & Medicaid Services to the possibility of fraudulent claims involving specific providers to adequately address this potential risk or other risks, different from those experienced to date.

Obtaining up-to-date contact information. VA's procedures for incident response and notification do not include mechanisms for obtaining contact information on individuals (when necessary), which can also cause delays in sending out notification letters to individuals. A VA official noted that notification letters to individuals could be delayed, depending on whether the department could locate complete address information for the affected individuals and on the number of letters that must be sent. Such delays occurred in the case of the missing backup tape in May 2006 (when 159 days passed before notification letters were sent). The data and number of records that were on the backup tape were not immediately known, and the address information of veterans whose data were compromised in the incident had to be researched. Our recent report noted that agencies faced challenges in identifying address information for individuals affected by security incidents and that mechanisms should be in place to obtain contact information on individuals.[27] However, VA's draft and approved interim procedures do not include a mechanism for obtaining such contact information. As a result, the department's response to incidents could be delayed when the compromised data do not include

[27] GAO, *Privacy: Lessons Learned about Data Breach Notification,* GAO-07-657 (Washington, D.C.: Apr. 30, 2007).

complete and accurate contact information (or there is uncertainty about the data).

Risk analysis. As mentioned earlier, VA asked the Department of Health and Human Services to conduct an independent risk analysis on the provider data loss in the January 2007 incident in Birmingham; this analysis showed that there was a high risk that the loss of personal information could result in harm to the individuals concerned. Conducting such risk analyses after incidents is a recommended procedure, since appropriate incident response and notification depend on determining the level of risk associated with the particular information that is compromised.[28] In addition, conducting periodic risk assessments before an incident occurs facilitates a rapid response, by enabling the development of mitigation activities and appropriate coordination for potential data losses. Assessments of both systems and the information they contain are important, particularly information with a high potential risk for inappropriate use or fraud. However, VA is still in the process of finalizing and approving its guidance for completing risk assessments on VA's systems. As a result, the department does not have a current assessment of risk for the information located at its facilities and in its information systems, which could affect the coordination and mitigation activities that are developed by the department to respond to potential data losses. Until VA assesses the risk for information located at its facilities and in its information systems and uses this assessment to develop and document mitigation activities and appropriate coordination for potential data losses (particularly high-risk losses), it may not be able to adequately address potential risks associated with loss of sensitive information at its facilities and on its systems.

Additional VA actions. VA has taken additional actions to improve incident response and notification. In February 2007, VA chartered the Incident Resolution Team Structure, a group of officials from organizations within the department who are responsible for responding to incidents and handling notification requirements at the national,

[28] We and the IG have issued reports that make recommendations for conducting risk assessments of high risk data for identity theft and determining if credit monitoring services or other appropriate services should be offered. See GAO, *Privacy: Lessons Learned about Data Breach Notification*, GAO-07-657 (Washington, D.C.: Apr. 30, 2007); Department of Veterans Affairs Office of Inspector General, *Administrative Investigation Loss of VA Information VA Medical Center Birmingham, AL*, Report No. 07-01083-157 (Washington, D.C.: June 29, 2007).

regional, and local levels. This action was in response to an OMB memorandum issued in September 2006, which recommended that all departments and agencies develop a core management group responsible for incident response to losses of personal information, as well as a response plan for notifying individuals affected by security incidents. Roles and responsibilities within the Incident Resolution Team Structure are organized according to the level of activity, the nature of the incident, and how the incident is categorized based on risk levels. VA also uses the Formal Event Review and Evaluation Tool to determine what the risk category of a security incident should be, based on the severity of the incident.

VA has also recently developed, with contractor assistance, interim regulations for security incident notification, data mining, fraud alerts, data breach analysis (that is, risk analysis of security incidents), credit monitoring, identity theft insurance, and credit protection services, as required under the Veterans Benefits, Health Care, and Information Technology Act of 2006. These interim regulations were approved by OMB and became effective on June 22, 2007.

Establishment of Office of IT Oversight and Compliance

According to *Standards for Internal Control in the Federal Government*,[29] internal controls at agencies should generally be designed to ensure that ongoing monitoring occurs in the course of normal operations. The methodology for evaluating an agency's internal controls should be logical and appropriate and may include assessments using checklists or other tools, as well as a review of the control design and direct testing of the internal control. The evaluation team should develop a plan for the evaluation process to ensure a coordinated effort, analyze the results of evaluation against established criteria, and ensure that the process is properly documented. The agency should also ensure that corrective action is taken within established time frames and is followed up on to verify implementation.

In an effort to promote internal controls within VA's computer environment, VA has consolidated a number of IT compliance programs

[29] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999). GAO also issued a management evaluation tool to assist agencies in maintaining or implementing effective internal control. See GAO, *Internal Control Management and Evaluation Tool*, GAO-01-1008G (Washington, D.C.: August 2001).

under one organization, the Office of IT Oversight and Compliance (ITOC). This office was established in January 2007. Previously, the Review and Inspection Division was responsible for conducting facility assessments and validating information entered into a database in response to VA's annual FISMA self-assessment survey. The division was incorporated into the ITOC, which is now responsible for providing independent, objective, and quality oversight and compliance services in the areas of cyber security, records management, and privacy. It is also responsible for conducting assessments of VA's facilities that (1) determine the adequacy of internal controls; (2) investigate compliance with laws, policies, and directives from VA and external organizations; and (3) ensure that proper safeguards are maintained. The results of these assessments are reported directly to the CIO and responsible supervisors at the facilities. The ITOC recommends corrective actions to remediate identified issues where necessary and also makes available a remediation team to assist the facility in addressing any recommendations. In January 2007, the ITOC began conducting assessments at facilities and by June 2007 had conducted 34 assessments. According to the Director of the ITOC, it recently became fully staffed with 127 personnel and will begin to conduct 12 to 18 assessments per month. VA facilities will be assessed every 3 years.

Although the ITOC was formed to identify security weaknesses and ensure compliance with federal law and department policy, its approach to conducting assessments does not include basic elements necessary for evaluating and monitoring controls. For example, although the ITOC developed a checklist to conduct facility assessments,[30] it did not develop a standard methodology for analysts to use when evaluating internal controls against the checklist, or specific criteria for each checklist item. As a result, the office lacks a process to ensure that its examination of internal controls is consistent across VA facilities. In addition, although the Director of the ITOC indicated that the assessment team recommendations to facilities are tracked in a database, no supporting documentation was provided. Further, according to the standards for internal control, organizations should follow up to ensure that corrective active is taken. However, the ITOC follows up to see if recommendations have been implemented only when a site is re-inspected. As a result, the

[30] The checklist is based on existing National Institute of Standards and Technology checklists and incorporates an assessment of internal controls and adherence to federal laws and VA policies.

office has no timely mechanism in place to ensure that its recommendations have been addressed. Until there are a standard methodology and established criteria for evaluating internal controls at facilities, as well as a mechanism in place to track recommendations and conduct regular follow-up on their status, VA will have limited assurance that its process for assessing its statutory and regulatory compliance and the effectiveness of its internal controls process is adequate and consistent across its facilities.

Conclusions

Effective information security controls are critical to securing the information systems and information on which VA depends to carry out its mission. GAO and IG recommendations to address long-standing weaknesses within the department have not yet been fully implemented, nor is the implementation of the IG recommendations expected to be completed in the near future. Consequently, there is an increased risk that personal information of veterans and other individuals, such as medical providers, will be exposed to potential data tampering, disruptions in critical operations, fraud, and the inappropriate disclosure of sensitive information. Until VA addresses recommendations to resolve identified weaknesses, it will have limited assurance that it can adequately protect its systems and information.

Although VA has begun or continued several initiatives to strengthen information security practices within the department, the shortcomings with the implementation of these initiatives could limit their effectiveness. If the department develops and documents processes, policies, and procedures; fills a key position and completes the implementation of major initiatives, then it will help ensure that these initiatives strengthen information security practices within the department. Sustained management commitment and oversight are vital to ensure the effective development, implementation, and monitoring of the initiatives that are being undertaken. Such involvement and oversight are critical to providing VA with a solid foundation for resolving long-standing information security weaknesses and continuously managing information security risks.

Recommendations for Executive Action

To assist the department in improving its ability to protect its information and systems, we are recommending the Secretary of Veterans Affairs take the following 17 actions:

- Finalize and approve Handbook 6500 to provide guidance for developing, documenting, and implementing the elements of the information security program.

- Develop, document, and implement a process for reviewing on a regular basis the performance plans of senior executives to ensure that information security is included as an evaluation element.

- Develop, document, and implement a process for the Director of Field Operations and Security and Director of Cyber Security to coordinate with each other on the implementation of IT security policies and procedures throughout the department.

- Document clearly defined responsibilities in the organization book for the Director of Field Operations and Security and the Director of Cyber Security for coordinating the implementation of IT security policies and procedures within the department.

- Act expeditiously to fill the position of the Chief Information Security Officer.

- Revise Directive 6500 to reflect the new IT management structure and to ensure that roles and responsibilities are consistent in all VA IT directives.

- Develop, document, and implement procedures for the action plan to ensure that action items are addressed in an effective and timely manner.

- Establish tasks with time frames for implementation of policies and procedures in the action plan.

- Develop, document, and implement a process to validate the closure of action plan items.

- Include in the action plan the activities taken to address GAO recommendations.

- Develop, document, and implement clear guidance for identifying devices that require encryption functionality.

- Maintain an accurate inventory of all IT equipment that has encryption installed.

- Develop and document procedures that include a mechanism for obtaining contact information on individuals whose information is compromised in security incidents.

- Conduct an assessment of what constitutes high-risk data for the information located at VA facilities and in information systems.

- Develop and document a process for appropriate coordination and mitigation activities based on the assessment above.

- Develop, document, and implement a standard methodology and established criteria for evaluating the internal controls at facilities.

- Establish a mechanism to track ITOC recommendations made to facilities and conduct regular follow-up on the status of the recommendations.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Deputy Secretary of Veterans Affairs (these are reprinted in appendix IV). The Deputy Secretary generally agreed with our findings and recommendations and stated that VA has already implemented or is working to implement all 17 recommendations. Additionally, the Deputy Secretary stated that the consolidation of all IT operations and maintenance under VA's Chief Information Officer will enhance the department's information security program, as well as correct long-standing deficiencies.[31]

In his comments, the Deputy Secretary also noted that the recommendation related to information security as an evaluation element in senior executive performance plans has already been implemented and that the recruitment announcement to fill the position of Chief Information Security Officer closed on July 27, 2007. He further stated that VA's Directive 6500, issued in August 2006, remains valid. However, as mentioned in our report, Directive 6500 was not updated to reflect the new IT realignment structure that was approved by the Secretary in February 2007 and roles and responsibilities should be consistent in all department policies and directives. The Deputy Secretary also discussed some of the activities that were underway to implement our recommendations.

[31] The Deputy Secretary also stated that VA considers its information security practices, as implemented before the May 2006 incident, as legally adequate, referring to the Government's response to litigation concerning the incident. However, our review did not assess the legal adequacy of the Department's safeguards in satisfying the Privacy Act, the statute involved in the litigation and to which the Deputy Secretary referred.

In the draft report that was provided for comment, we indicated that VA had not implemented any of the IG's 22 recommendations to improve information security. We have since received new information and have updated the report to reflect that VA has now implemented 2 of the 22 IG recommendations.

As agreed, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we are sending copies of this report to interested congressional committees; the Secretary of Veterans Affairs; and other interested parties. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at www.gao.gov.

If you have any questions regarding this report, please contact me at (202) 512-6244 or by e-mail at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix V.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

List of Requesters

The Honorable Harry Reid
Majority Leader
United States Senate

The Honorable Daniel K. Akaka
Chairman
Committee on Veterans' Affairs
United States Senate

The Honorable Bob Filner
Chairman
Committee on Veterans' Affairs
House of Representatives

The Honorable Hillary Rodham Clinton
United States Senate

The Honorable Byron L. Dorgan
United States Senate

The Honorable Joseph I. Lieberman
United States Senate

The Honorable Patty Murray
United States Senate

The Honorable Barack Obama
United States Senate

The Honorable John D. Rockefeller IV
United States Senate

The Honorable Ken Salazar
United States Senate

The Honorable Charles E. Schumer
United States Senate

Appendix I: Objectives, Scope, and Methodology

Our objectives were to evaluate (1) whether the Department of Veterans Affairs (VA) has effectively addressed GAO and VA Office of Inspector General (IG) recommendations to strengthen its information security practices and (2) actions VA has taken since the May 2006 security incident to strengthen its information security practices and secure personal information. In doing this work, we analyzed relevant documentation including policies, procedures, and plans, and interviewed key department officials in Washington, D.C., to identify and assess VA's progress in implementing recommendations and federal legislation to strengthen its information security practices. We also drew on previous GAO reports and testimonies, as well as on expert opinion provided in congressional testimony and other sources. We used certain applicable federal laws, other requirements, and guidelines, including Office of Management and Budget (OMB) memorandums, in assessing whether the Department's actions and initiatives can help ensure departmental compliance.

For the first objective, we evaluated VA's actions to address GAO and VA IG recommendations, respectively in our 2002 report and in the IG's July 2006 and September 2006 reports. To review VA's history of implementation efforts, we examined GAO reports, testimony from recent congressional hearings made by GAO and IG staff, as well as reports by the VA IG. To determine the implementation status of open GAO recommendations, we analyzed pertinent security policies, procedures, and plans and met with officials from VA to gather information on the department's actions to address the recommendations. To determine the implementation status of open IG recommendations we met with officials from the VA IG Office of Audit to discuss the status of these recommendations and met with VA officials to learn what actions had been taken or were planned to take to fully address the recommendations.[1] The VA IG concurred with the status information provided.

For the second objective, we evaluated VA's actions to strengthen its information security practices to comply with federal guidance, including recent OMB memorandums. We met with department officials to gather information on what initiatives VA had undertaken or planned to undertake to improve its information security practices. For each initiative, we obtained and analyzed supporting documentation and met

[1] The IG evaluated VA's actions in addressing recommendations made by the IG as part of their annual FISMA review during fiscal year 2006.

with department officials responsible for the implementation of the initiatives to assess the extent to which the department had complied with federal requirements and other guidelines. In addition, we also performed audit procedures to determine the extent to which VA has installed encryption functionality on its laptop computers. Our detailed scope and methodology for the laptop encryption testing are below.

Laptop Encryption Testing

We examined 248 laptops at eight locations to determine whether encryption software had been installed on a selection of laptops as indicated by VA.

Selection of Locations

We selected the locations to be visited based on (1) the type of facility[2] and (2) number of facilities available to be tested in a geographic area. We identified different facility types in proximity to each other and to GAO offices. Clinics and cemeteries were excluded from the selection because the number of laptops at these locations would be quite small. We also selected a Research Enhancement Award Program location based on an incident in January 2007 involving this type of location. On the basis of the criteria listed above, we selected the following eight facilities: Baltimore Regional Office, Chicago Regional Office, Denver Health Administration Center, Denver Regional Office, Denver Research Enhancement Award Program, Hines Data Center, Hines Medical Center and the Washington, D.C., Medical Center.

Selection of Laptops

At each location, we obtained an inventory or population of “in use” laptops. We examined every laptop in the population that was available for review at the Baltimore Regional Office, Chicago Regional Office, Denver Research Enhancement Award Program, and the Hines Data Center because of the relatively small number of laptops in the population. We selected random samples of laptops with the intent of projecting the results to each population at the Denver Health Administration Center, Denver Regional Office, Hines Medical Center, and Washington, D.C., Medical Center.[3]

[2] The types of VA facilities include central and regional offices, data centers, medical centers, clinics, Research Enhancement Award Program offices, and cemeteries.

[3] With these probability samples, each laptop had a known, nonzero probability of being selected.

Testing of Laptops

We conducted testing of encryption implementation on laptops at select VA facilities to determine whether the department's laptops were in compliance with VA Directive 6504 which stated that if a laptop was in a mobile environment and contained sensitive information that it be encrypted using approved software that is validated against National Institute of Standards and Technology standards. We also tested laptops at the two medical facilities to see whether the laptops should be encrypted according to the facility inventory because multiple inventories were received from these locations. In addition, we tested the laptops at the two medical facilities to see whether the laptop was considered a medical device based on the definition of medical devices provided to us by VA. At each location there were a small number of laptops that were unavailable to us to be tested. Department officials cited several reasons for this, including that the laptop had been turned in to be disposed of or discarded according to VA policy, had a hard drive failure, or could not be brought in to the site for testing. In table 3, the "laptops tested" column represents the number of laptops the team was able to test.

Table 3: Number of Laptops Tested at Select VA Facilities

Location	Laptops in population	Laptops tested
Baltimore Regional Office	18	15
Chicago Regional Office	27	23
Denver Health Administration Center	82	37
Denver Regional Office	42	27
Denver Research Enhancement Award Program	25	21
Hines Data Center	29	26
Hines Medical Center	313	41
Washington, D.C., Medical Center	357	58
Total	**893**	**248**

Source: GAO analysis.

Analysis of Results

For all four locations where every laptop in the population was tested, we used the results of our test to determine whether the directive had been consistently implemented. For the Denver Health Administration Center and the Denver Regional Office, our sample results allowed us to estimate with 95 percent confidence that at least 93 percent of the laptops would have consistently implemented the directive.[4] On the basis of these results, we concluded that at these six sites, VA had consistently implemented its directive. For the Hines Medical Center and the Washington, D.C., Medical Center, the results of our tests indicated that VA's directive had not been consistently implemented for one laptop and three laptops at these facilities respectively.

We performed our work at VA headquarters in Washington, D.C., and at the selected VA facilities listed above, in accordance with generally accepted government auditing standards, from November 2006 through August 2007.

[4] Because we selected a sample of laptops from these locations, our results are estimates of the populations and thus are subject to sample errors that are associated with samples of this size and type. Our confidence in the precision of the results from this sample is expressed in 95 percent confidence intervals, which are expected to include the actual results in 95 percent of the samples of this type.

Appendix II: Status of Prior VA IG Recommendations

This appendix includes the actions the Department of Veterans Affairs (VA) has taken or is planning to take to address 17 recommendations related to Federal Information Security Management Act related findings made by the VA Office of Inspector General (IG)[1] as reported to us by the completion of our review in August 2007.

Table 4: Status of 17 VA IG Recommendations Related to FISMA Findings

VA IG recommendations	Status	Actions taken or planned
Implement a centralized information technology (IT) management approach; apply appropriate resources; establish, clarify, and modify IT policies and procedures pursuant to organizational changes; and implement and enforce security controls.	Open	The new organization structure was approved by the Secretary in February 2007. Business processes and IT governance are to be developed following the approval. VA is also in the process of developing policies and procedures for the organizational changes, including a department strategic plan, and incorporating security into capital planning and investment control processes and information security officer management and operating procedures. Of these, the majority were supposed to be finished by June 2007 but are still in the midst of completion.
Develop and implement solutions for the establishment of a patch management program.	Open	VA will complete its implementation of a patch management program by the end of December 2009, including the development of a central patch management policy and establishing a patch management configuration standard.
Identify and implement solutions for resolving access control vulnerabilities, ensure segregation of duties, remind all sites to confirm virus protection files are updated prior to authorizing connection to their networks, and resolve all self-reported access control weaknesses.	Open	VA is developing criteria for authorizing access to IT systems and a directive on access controls, both of which are scheduled to be completed in August 2007. VA is also making enhancements to its antivirus program, planned to be completed in March 2008.
Review and update all applicable position descriptions to better describe sensitivity ratings, better document employee personnel records and contractor files to include signed "Rules of Behavior" instructions, annual certifications of veterans' statuses, annual privacy and Health Insurance Portability and Accountability Act training certifications, and position sensitivity level designations.	Open	VA is refining and standardizing IT position descriptions, updating risk designations, and revising the table of penalties (includes examples of disciplinary action for violations). Of these activities, all have missed their deadline for completion and work still remains to be performed. VA will also conduct a review to ensure the position descriptions that are being refined and updated are consistent across the department. This will be undertaken in October 2008.
Timely request the appropriate level of background investigations on all applicable employees and contractors. Additionally, monitor and ensure timely requests for reinvestigations on all applicable employees and contractors.	Open	VA is in the process of completing any additional background investigations that may be needed. VA is also implementing the use of an Office of Personnel Management-sponsored system that will allow electronic completion and submission of all personnel investigation forms for completion of the investigations. This was scheduled to be completed in May 2007 but work has not yet begun on the task.

[1] Department of Veterans Affairs Office of Inspector General, *FY2005 Audit of VA Information Security Program*, Report No. 05-00055-216 (Washington, D.C.: Sept. 20, 2006).

VA IG recommendations	Status	Actions taken or planned
Provide the IG with the results of researching the benefits and costs of deploying intrusion prevention systems at all sites.	Closed[a]	VA is also in the process of installing a host-based intrusion prevention system for its servers as both prudent and necessary without a cost benefit analysis and that they will be replacing intrusion detection system equipment with intrusion prevention system equipment.
Continue efforts to strengthen critical infrastructure planning, complete the Infrastructure Protection Plan, and ensure infrastructure planning addresses other information security requirements.	Open	VA is developing a Critical Infrastructure Protection Plan that is planned for completion in January 2008. VA is also planning to acquire an IT asset tracking system; utilizing the system, it will inventory all IT equipment throughout the department. These activities have not yet begun but are scheduled for completion in October 2009.
Collaboratively test Information Technology Centers' continuity of operations plans in a joint effort with all tenant groups (Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), National Cemetery Administration, and other program offices) to ensure that backup sites will support all mission related operations, and report test results to the IG for further review.	Open	The department is currently developing a network and security operations center continuity of operations plan but the completion deadline of March 2007 has been missed and work still remains. VA is also developing a directive for contingency planning that is scheduled to be completed in August 2007.
Address all self-reported deficiencies identified as the result of completed certification and accreditation's and related review work.	Open	VA is currently in the process of developing criteria for system control testing, and this process is scheduled to be completed in August 2007. VA is also reviewing its guidance on certification and accreditation and will conduct recertification of all its systems, including its regional data centers, in the summer of 2008.
Determine the extent to which uncertified Internet gateways continue to exist, and take actions to terminate and upgrade external connections susceptible to inappropriate access.	Open	VA is currently enhancing controls at network boundaries, though the completion deadline of June 2007 has been missed. It is also developing a process to require authorization prior to connecting to non-VA systems that is planned to be completed in October 2007.
Improve configuration management practices by identifying, replacing, or justifying the continuance of older operating systems that are vulnerable to security breaches.	Open	VA is currently developing criteria for documenting and controlling information system changes, and procedures for enforcing access restrictions on the ability to change a system. It is also upgrading its systems to Windows XP and work is expected to be completed by September 2007. The department also plans to develop a national change control policy, though work has not yet begun.
Complete actions to relocate and consolidate VA Central Office's Data Center.	Closed[a]	VA completed activities to move and consolidate the VA Central Office data center by relocating servers and network hardware to other VA locations.
Develop and implement VA-wide application program/operating system change control procedures to ensure consistent documentation and authorization practices are deployed at all facilities.	Open	VA is currently working on improving application and operating system change controls and establishing an enterprise change control board. Both activities are planned to be completed in December 2007.
Strengthen physical access controls to correct previously reported physical access control deficiencies and develop consistent standardized physical access control requirements, policies, and guidelines throughout VA.	Open	VA is currently in the process of developing a directive for physical and environmental protection; this process is planned for completion in August 2007. It is in the process of restricting physical access to computer rooms, though work was scheduled to be completed in January 2007.

VA IG recommendations	Status	Actions taken or planned
Reduce wireless security vulnerabilities by ensuring sites have an effective and up-to-date methodology to protect the interception of wireless signals and accessing the network. Additionally, ensure the wireless network is segmented and protected from the wired network.	Open	VA is in the process of establishing regular update mechanisms for security configuration on those devices, though actions were planned for completion by May 2007. VA is also developing standards for restricting the use of mobile and portable devices that are planned for completion in August 2007.
Identify and deploy solutions to encrypt sensitive data and resolve clear text protocol vulnerabilities.	Open	VA announced that it had encrypted 18,000 laptops by September 15, 2006. VA is currently developing management criteria for public key infrastructure tokens and criteria for revoking or changing the tokens and standards for transporting media outside of VA, though work was scheduled for completion by July 2007.
Conduct validation tests in conjunction with remediation efforts to ensure all information and data retained in the Security Management and Reporting Tool database is accurate, complete, and reliable.	Open	VA is currently working to enhance the Security Management and Reporting Tool database with modules for certification and accreditation, risk management, and reviews and inspections, this work was scheduled for completion in June 2007, though work remains to be completed.

Source: GAO analysis of VA action plan.

[a] The VA IG stated that VA's actions to resolve this recommendation are sufficient to close the recommendation.

Appendix III: Information on Selected Security Incidents at VA from December 2003 to January 2007

The Department of Veterans Affairs (VA) had at least 1500 security incidents reported between December 2003 and January 2007 which included the loss of personal information. Below is additional information on a selection of incidents, including all publicly reported incidents subsequent to May 3, 2006, that were reported to the department during this period and what actions it took to respond to these incidents. These incidents were selected from data obtained from VA to provide illustrative examples of the incidents that occurred at the department during this period.

- *December 9, 2003: stolen hard drive with data on 100 appellants.* A VA laptop computer with benefit information on 100 appellants was stolen from the home of an employee working at home. As a result, the agency office was going to recall all laptop computers and have encryption software installed by December 23, 2003.

- *November 24, 2004: unintended disclosure of personal information.* A public drive on a VA e-mail system permitted entry to folders/files containing veterans' personal information (names, Social Security numbers, dates of birth, and in some cases personal health information such as surgery schedules, diagnosis, status, etc.) by all users after computer system changes made. All folders were restricted, and individual services were contacted to set up limited access lists.

- *December 6, 2004: two personal computers containing data on 2,000 patients stolen.* Two desktop personal computers were stolen from a locked office in a research office of a medical center. One of the computers had files containing names, Social Security numbers, next of kin, addresses, and phone numbers of approximately 2,000 patients. The computers were password protected by the standard VA password system. The medical center immediately contacted the agency Privacy Officer for guidance. Letters were mailed to all research subjects informing them of the computer theft and potential for identity theft. VA enclosed letters addressed to three major credit agencies and postage paid envelopes. This incident was reported to VA and federal incident offices.

- *March 4, 2005: list of 897 providers' Social Security numbers sent via e-mail.* An individual reported e-mailing a list of 897 providers' names and Social Security numbers to a new transcription company. This was immediately reported, and the supervisor called the transcription company and spoke with the owner and requested that the file be destroyed immediately. Notification letters were sent out to all 897 providers. Disciplinary action was taken against the employee.

- *October 14, 2005: personal computer containing data on 421 patients stolen.* A personal computer that contained information on 421 patients was stolen from a medical center. The information on the computer included patients' names; the last four digits of their Social Security numbers; and their height, weight, allergies, medications, recent lab results, and diagnoses. The agency's Privacy Officer and medical center information security officer were notified. The use of credit monitoring was investigated, and it was determined that because the entire Social Security number was not listed, it would not be necessary to use these services at the time.

- *February 2, 2006: inappropriate access of VA staff medical records.* A VA staff member accessed several coworkers' medical records to find date of birth. Employee information was compromised and several records were accessed on more than one occasion. No resolution recorded.

- *April 11, 2006: suspected hacker compromised systems with employee's assistance.* A former VA employee is suspected of hacking into a medical center computer system with the assistance of a current employee providing rotating administrator passwords. All systems in the medical center serving 79,000 veterans were compromised.

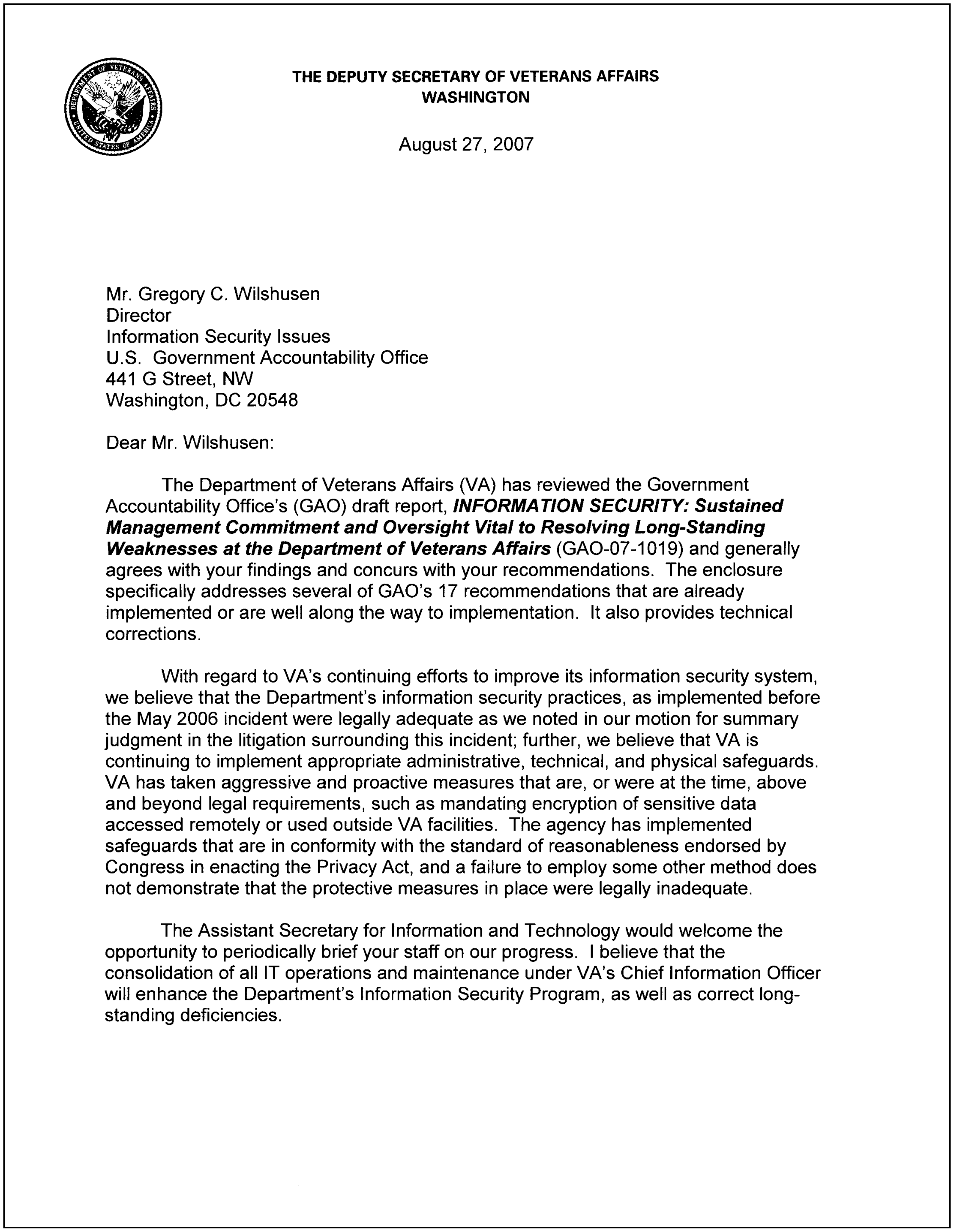
- *May 5, 2006: missing backup tape with sensitive information on 7,052 individuals.* An office determined it was missing a backup tape containing sensitive information. On June 29, 2006, it was reported that approximately 7,052 veterans were affected by the incident. On October 11, 2006, notification letters were mailed, and 5,000 veterans received credit protection and data breach analysis for 2 years.

- *August 3, 2006: desktop computer with approximately 18,000 patient financial records stolen.* A desktop computer was stolen from a secured area at a contractor facility in Virginia that processes financial accounts for VA. The desktop computer was not encrypted. Notification letters were mailed and credit monitoring services offered.

- *September 6, 2006: laptop with patient information on an unknown number of individuals stolen.* A laptop attached to a medical device at a VA medical center was stolen. It contained patient information on an unknown number of individuals. Notification letters and credit protection services were offered to 1,575 patients.

- *January 22, 2007: external hard drive with 535,000 individual records and 1.3 million non-VA physician provider records missing* *or stolen.* An external hard drive used to store research data with 535,000 individual records and 1.3 million non-VA physician provider records was discovered missing or stolen from a research facility in Birmingham, Alabama. Notification letters were sent to veterans and providers, and credit monitoring services were offered to those individuals whose records contained personally identifiable information.

Appendix IV: Comments from the Department of Veterans Affairs



THE DEPUTY SECRETARY OF VETERANS AFFAIRS
WASHINGTON

August 27, 2007

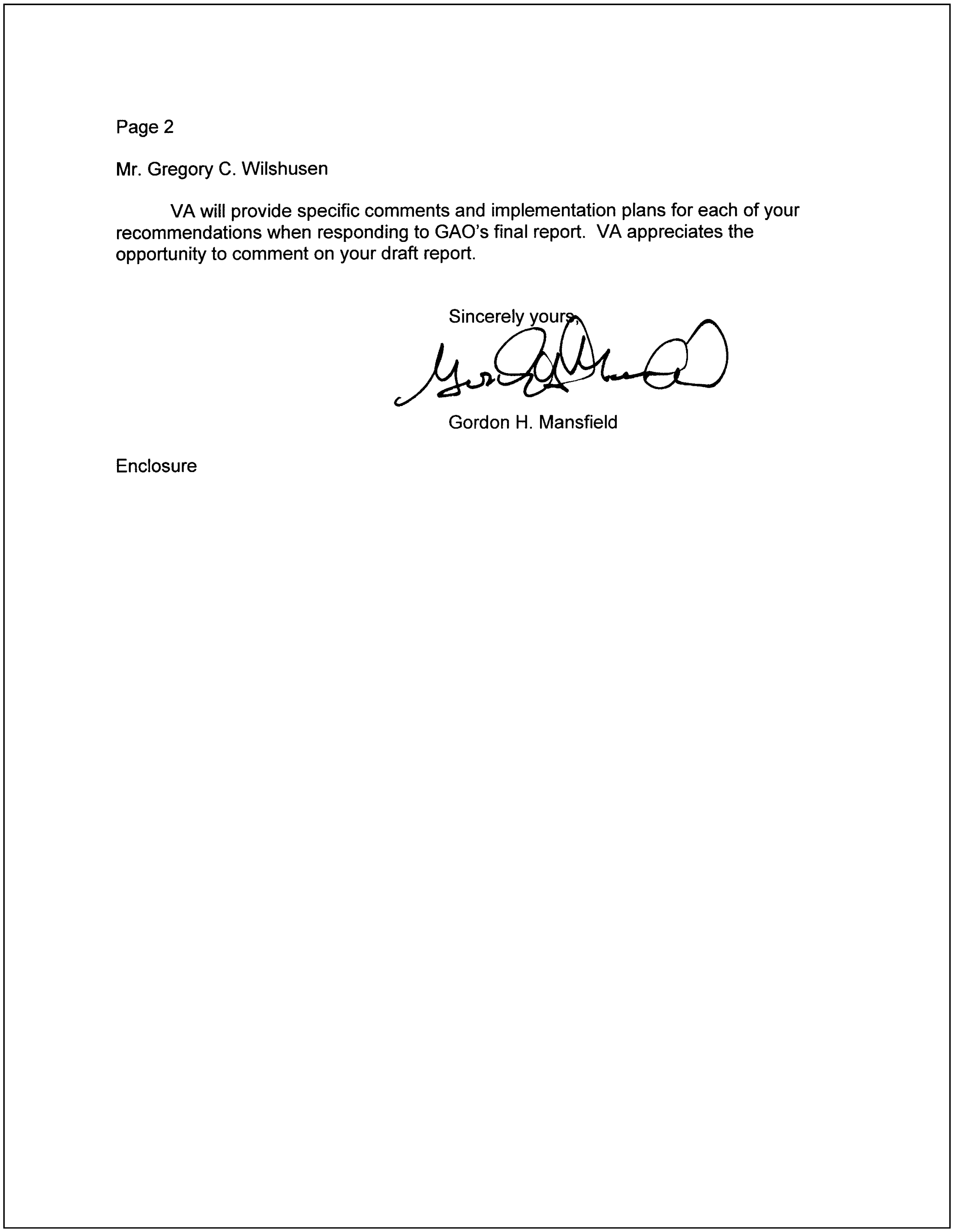
Mr. Gregory C. Wilshusen
Director
Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, ***INFORMATION SECURITY: Sustained Management Commitment and Oversight Vital to Resolving Long-Standing Weaknesses at the Department of Veterans Affairs*** (GAO-07-1019) and generally agrees with your findings and concurs with your recommendations. The enclosure specifically addresses several of GAO's 17 recommendations that are already implemented or are well along the way to implementation. It also provides technical corrections.

With regard to VA's continuing efforts to improve its information security system, we believe that the Department's information security practices, as implemented before the May 2006 incident were legally adequate as we noted in our motion for summary judgment in the litigation surrounding this incident; further, we believe that VA is continuing to implement appropriate administrative, technical, and physical safeguards. VA has taken aggressive and proactive measures that are, or were at the time, above and beyond legal requirements, such as mandating encryption of sensitive data accessed remotely or used outside VA facilities. The agency has implemented safeguards that are in conformity with the standard of reasonableness endorsed by Congress in enacting the Privacy Act, and a failure to employ some other method does not demonstrate that the protective measures in place were legally inadequate.

The Assistant Secretary for Information and Technology would welcome the opportunity to periodically brief your staff on our progress. I believe that the consolidation of all IT operations and maintenance under VA's Chief Information Officer will enhance the Department's Information Security Program, as well as correct long-standing deficiencies.



Page 2

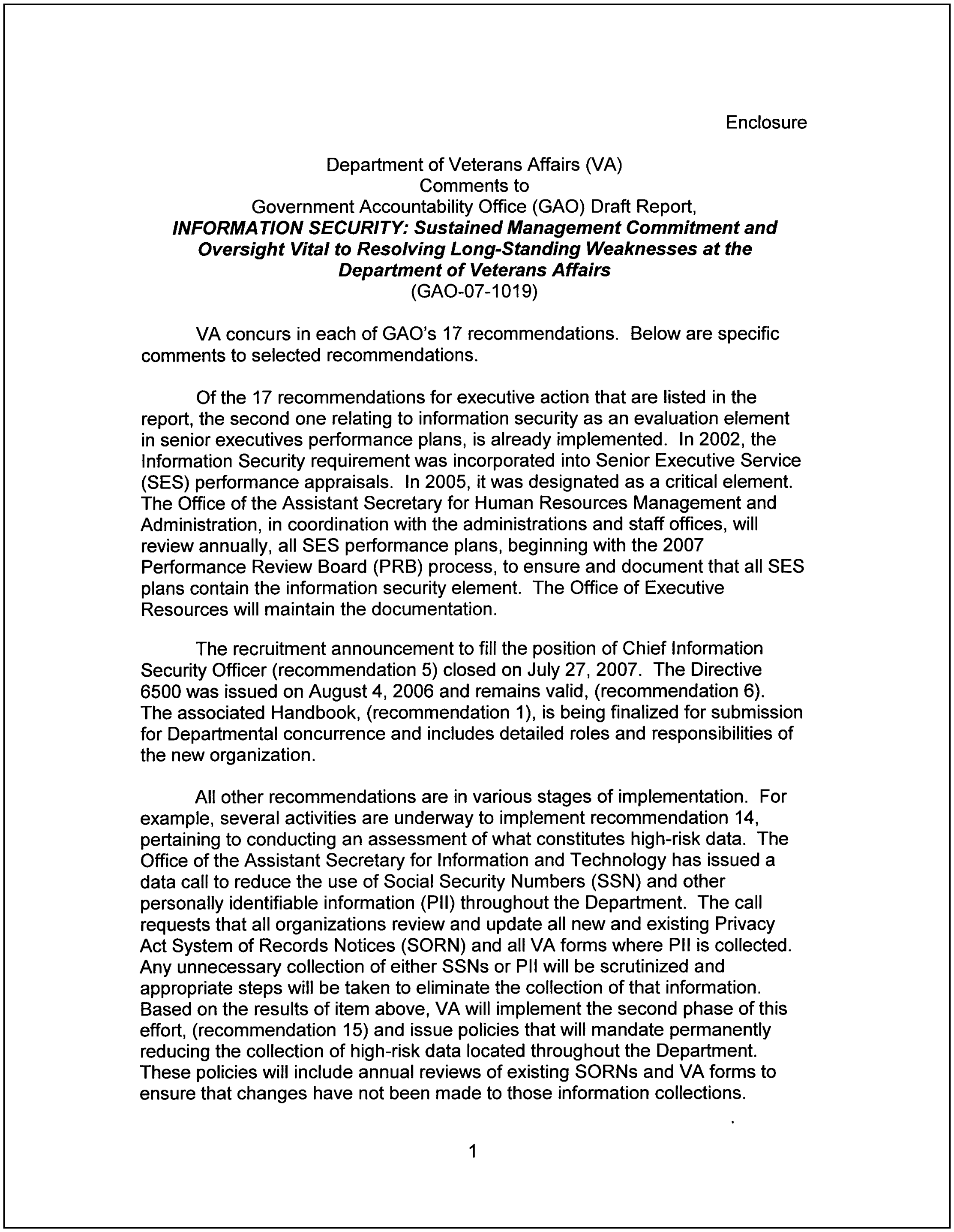
Mr. Gregory C. Wilshusen

VA will provide specific comments and implementation plans for each of your recommendations when responding to GAO's final report. VA appreciates the opportunity to comment on your draft report.

Sincerely yours,

Gordon H. Mansfield

Enclosure



Enclosure

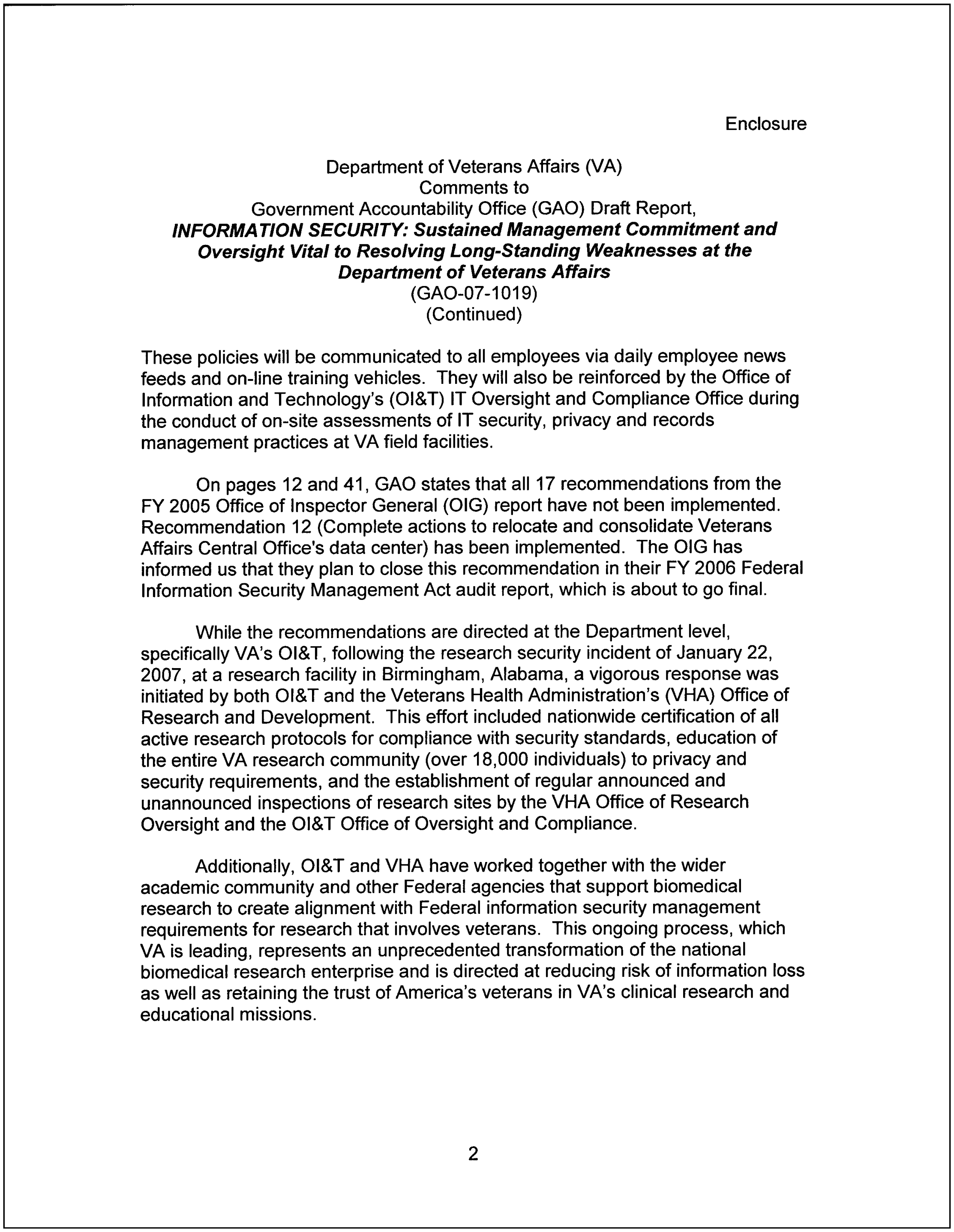
Department of Veterans Affairs (VA)
Comments to
Government Accountability Office (GAO) Draft Report,
INFORMATION SECURITY: Sustained Management Commitment and Oversight Vital to Resolving Long-Standing Weaknesses at the Department of Veterans Affairs
(GAO-07-1019)

VA concurs in each of GAO's 17 recommendations. Below are specific comments to selected recommendations.

Of the 17 recommendations for executive action that are listed in the report, the second one relating to information security as an evaluation element in senior executives performance plans, is already implemented. In 2002, the Information Security requirement was incorporated into Senior Executive Service (SES) performance appraisals. In 2005, it was designated as a critical element. The Office of the Assistant Secretary for Human Resources Management and Administration, in coordination with the administrations and staff offices, will review annually, all SES performance plans, beginning with the 2007 Performance Review Board (PRB) process, to ensure and document that all SES plans contain the information security element. The Office of Executive Resources will maintain the documentation.

The recruitment announcement to fill the position of Chief Information Security Officer (recommendation 5) closed on July 27, 2007. The Directive 6500 was issued on August 4, 2006 and remains valid, (recommendation 6). The associated Handbook, (recommendation 1), is being finalized for submission for Departmental concurrence and includes detailed roles and responsibilities of the new organization.

All other recommendations are in various stages of implementation. For example, several activities are underway to implement recommendation 14, pertaining to conducting an assessment of what constitutes high-risk data. The Office of the Assistant Secretary for Information and Technology has issued a data call to reduce the use of Social Security Numbers (SSN) and other personally identifiable information (PII) throughout the Department. The call requests that all organizations review and update all new and existing Privacy Act System of Records Notices (SORN) and all VA forms where PII is collected. Any unnecessary collection of either SSNs or PII will be scrutinized and appropriate steps will be taken to eliminate the collection of that information. Based on the results of item above, VA will implement the second phase of this effort, (recommendation 15) and issue policies that will mandate permanently reducing the collection of high-risk data located throughout the Department. These policies will include annual reviews of existing SORNs and VA forms to ensure that changes have not been made to those information collections.



Enclosure

Department of Veterans Affairs (VA)
Comments to
Government Accountability Office (GAO) Draft Report,
INFORMATION SECURITY: Sustained Management Commitment and Oversight Vital to Resolving Long-Standing Weaknesses at the Department of Veterans Affairs
(GAO-07-1019)
(Continued)

These policies will be communicated to all employees via daily employee news feeds and on-line training vehicles. They will also be reinforced by the Office of Information and Technology's (OI&T) IT Oversight and Compliance Office during the conduct of on-site assessments of IT security, privacy and records management practices at VA field facilities.

On pages 12 and 41, GAO states that all 17 recommendations from the FY 2005 Office of Inspector General (OIG) report have not been implemented. Recommendation 12 (Complete actions to relocate and consolidate Veterans Affairs Central Office's data center) has been implemented. The OIG has informed us that they plan to close this recommendation in their FY 2006 Federal Information Security Management Act audit report, which is about to go final.

While the recommendations are directed at the Department level, specifically VA's OI&T, following the research security incident of January 22, 2007, at a research facility in Birmingham, Alabama, a vigorous response was initiated by both OI&T and the Veterans Health Administration's (VHA) Office of Research and Development. This effort included nationwide certification of all active research protocols for compliance with security standards, education of the entire VA research community (over 18,000 individuals) to privacy and security requirements, and the establishment of regular announced and unannounced inspections of research sites by the VHA Office of Research Oversight and the OI&T Office of Oversight and Compliance.

Additionally, OI&T and VHA have worked together with the wider academic community and other Federal agencies that support biomedical research to create alignment with Federal information security management requirements for research that involves veterans. This ongoing process, which VA is leading, represents an unprecedented transformation of the national biomedical research enterprise and is directed at reducing risk of information loss as well as retaining the trust of America's veterans in VA's clinical research and educational missions.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the individual named above, key contributions to this report were made by Charles Vrabel (Assistant Director), James Ashley, Mark Canter, Barbara Collier, Mary Hatcher, Valerie Hopkins, Leena Mathew, Jeanne Sung, and Amos Tevelow.

(310583)

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

Susan Becker, Acting Manager, Beckers@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER