United States Government Accountability Office

GAO

Testimony
Before the House Committee on Veterans' Affairs

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, September 26, 2007

VETERANS AFFAIRS

Sustained Management Commitment and Oversight Are Essential to Completing Information Technology Realignment and Strengthening Information Security

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

Gregory C. Wilshusen
Director, Information Security Issues

GAO-07-1264T

September 26, 2007

VETERANS AFFAIRS

Sustained Management Commitment and Oversight Are Essential to Completing Information Technology Realignment and Strengthening Information Security

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-1264T, a testimony before the House Committee on Veterans' Affairs

Why GAO Did This Study

The Department of Veterans Affairs (VA) has encountered numerous challenges in managing its information technology (IT) and securing its information systems. In October 2005, the department initiated a realignment of its IT program to provide greater authority and accountability over its resources. The May 2006 security incident highlighted the need for additional actions to secure personal information maintained in the department's systems.

In this testimony, GAO discusses its recent reporting on VA's realignment effort as well as actions to improve security over its information systems. To prepare this testimony, GAO reviewed its past work on the realignment and on information security, and it updated and supplemented its analysis with interviews of VA officials.

What GAO Recommends

In recent reports, GAO made recommendations aimed at improving VA's management of its realignment efforts and information security program.

What GAO Found

VA has fully addressed two of six critical success factors GAO identified as essential to a successful transformation, but it has yet to fully address the other four, and it has not kept to its scheduled timelines for implementing new management processes that are the foundation of the realignment. That is, the department has ensured commitment from top leadership and established a governance structure to manage resources, both of which are critical success factors. However, the department continues to operate without a single, dedicated implementation team to manage the realignment; such a dedicated team is important to oversee the further implementation of the realignment, which is not expected to be complete until July 2008. Other challenges to the success of the realignment include delays in staffing and in implementing improved IT management processes that are to address long-standing weaknesses. The department has not kept pace with its schedule for implementing these processes, having missed its original scheduled time frames. Unless VA dedicates a team to oversee the further implementation of the realignment, including defining and establishing the processes that will enable the department to address its IT management weaknesses, it risks delaying or missing the potential benefits of the realignment.

VA has begun or continued several major initiatives to strengthen information security practices and secure personally identifiable information within the department, but more remains to be done. These initiatives include continuing the department's efforts to reorganize its management structure; 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, although the management structure for information security has changed under the realignment, improved security management processes have not yet been completely developed and implemented, and responsibility for the department's information security functions is divided between two organizations, with no documented process for the two offices to coordinate with each other. In addition, VA has made limited progress in implementing prior security recommendations made by GAO and the department's Inspector General, having yet to implement 22 of 26 recommendations. Until the department addresses shortcomings in its major security initiatives and implements prior recommendations, it will have limited assurance that it can protect its systems and information from the unauthorized disclosure, misuse, or loss of personally identifiable information.

To view the full product, including the scope and methodology, click on GAO-07-1264T. For more information, contact Valerie Melvin at (202) 512-6304 or melvinv@gao.gov.

Mr. Chairman and Members of the Committee:

Thank you for inviting us to participate in today's hearing on the Department of Veterans Affairs (VA) realignment of its information technology management structure and actions toward strengthening its information security program. In carrying out its mission of serving our nation's veterans, the department relies heavily on information technology (IT), for which it expends about $1 billion annually. As you know, however, VA has encountered persistent challenges in IT management, having experienced cost, schedule, and performance problems in its information system initiatives, as well as losses of sensitive information contained in its systems. We have reported that a contributing factor to VA's challenges in managing projects and improving security was the department's management structure, which until recently was decentralized, giving the administrations[1] and headquarters offices[2] control over a majority of the department's IT budget.

In October 2005, VA initiated a realignment of its IT program to provide greater authority and accountability over its resources. In undertaking this realignment (due for completion in July 2008), the department's goals are to centralize IT management under the department-level Chief Information Officer (CIO) and standardize operations and the development of systems across the department through the use of new management processes based on industry best practices. This past June we reported on the department's realignment initiative, noting progress as well as the need for additional actions to be completed.[3] Just last week, we also released a report on VA information security, which included an assessment

[1]The VA comprises three administrations: the Veterans Benefits Administration, the Veterans Health Administration, and the National Cemetery Administration.

[2]The headquarters offices include the Office of the Secretary, six Assistant Secretaries, and three VA-level staff offices.

[3]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).

of the realignment with regard to the department's information security practices.[4]

At your request, my testimony today will summarize the department's actions to realign IT management and our findings regarding the department's information security program. In developing this testimony, we reviewed our previous work on the department's realignment and efforts to strengthen information security. We also obtained and analyzed pertinent documentation and supplemented our analysis with interviews of responsible VA officials to determine the current status of the department's realignment efforts. All work on which this testimony is based was conducted in accordance with generally accepted government auditing standards.

Results in Brief

VA has fully addressed two of six critical success factors we have identified as essential to a successful transformation, but it has not kept to its timelines for implementing new management processes that are the foundation of the realignment. Consequently, the department is in danger of not being able to meet its 2008 targeted completion date. The department has ensured commitment from top leadership and established a governance structure to manage resources, both of which are critical success factors. However, the department continues to operate without a single, dedicated implementation team to manage the realignment; such a dedicated team is important to oversee the further implementation of the realignment. Other challenges to the success of the realignment include delays in staffing and in implementing the IT management processes that are the foundation of the realignment. The department has not kept pace with its schedule for implementing these processes, having missed its original scheduled time frames.

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

Unless VA dedicates a team to oversee the further implementation of the realignment, including defining and establishing the processes that will enable the department to address its IT management weaknesses, it risks delaying or missing the potential benefits of the realignment.

VA has made progress in strengthening information security, but much work remains to resolve long-standing security weaknesses. The department has begun or has continued several major initiatives to strengthen information security practices and secure personally identifiable information[5] within the department. These initiatives include continuing the department's efforts, as described above, to realign its management structure; 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, a new security management structure has been implemented, but improved security management processes have not yet been completely developed and implemented; in addition, the new security management structure divides the responsibility for the department's information security functions between two organizations, with no documented process for the two offices to coordinate with each other. Further, the department has made limited progress in addressing prior GAO and Inspector General recommendations to improve security: although VA has taken steps to address these, it has not yet completed the implementation of 22 out of 26 prior recommendations.

In the reports covered by this testimony, we have made numerous recommendations aimed at improving the department's management of its realignment and information security program. VA has agreed with these recommendations and has begun taking or plans to take action to implement them. If this implementation is properly executed, it could help the department to realize the

[5]Personally identifiable information, which can be used to locate or identify an individual, includes things such as names, aliases, and Social Security numbers.

expected benefits of the realignment, as well as to better secure its information and systems.

Background

VA's mission is to promote the health, welfare, and dignity of all veterans in recognition of their service to the nation by ensuring that they receive medical care, benefits, social support, and lasting memorials. Over time, the use of IT has become increasingly crucial to the department's effort to provide benefits and services. VA relies on its systems for medical information and records for veterans, as well as for processing benefit claims, including compensation and pension and education benefits.

In reporting on VA's IT management over the past several years, we have highlighted challenges the department has faced in enabling its employees to help veterans obtain services and information more quickly and effectively while also safeguarding personally identifiable information. A major challenge was that the department's information systems and services were highly decentralized, giving the administrations a majority of the IT budget.[6] In addition, VA's policies and procedures for securing sensitive information needed to be improved and implemented consistently across the department.

As we have previously pointed out,[7] it is crucial for the department CIO to ensure that well-established and integrated processes for leading, managing, and controlling investments in information systems and programs are followed throughout the department. Similarly, a contractor's assessment of VA's IT organizational

[6]For example, according to an October 2005 memorandum from the former CIO to the Secretary of Veterans Affairs, the CIO had direct control over only 3 percent of the department's IT budget and 6 percent of the department's IT personnel. In addition, in the department's fiscal year 2006 IT budget request, the Veterans Health Administration was identified to receive 88 percent of the requested funding, while the department was identified to receive only 4 percent.

[7]GAO-07-844.

alignment, issued in February 2005, noted the lack of control over how and when money is spent.[8] The assessment noted that the focus of department-level management was only on reporting expenditures to the Office of Management and Budget and Congress, rather than on managing these expenditures within the department.

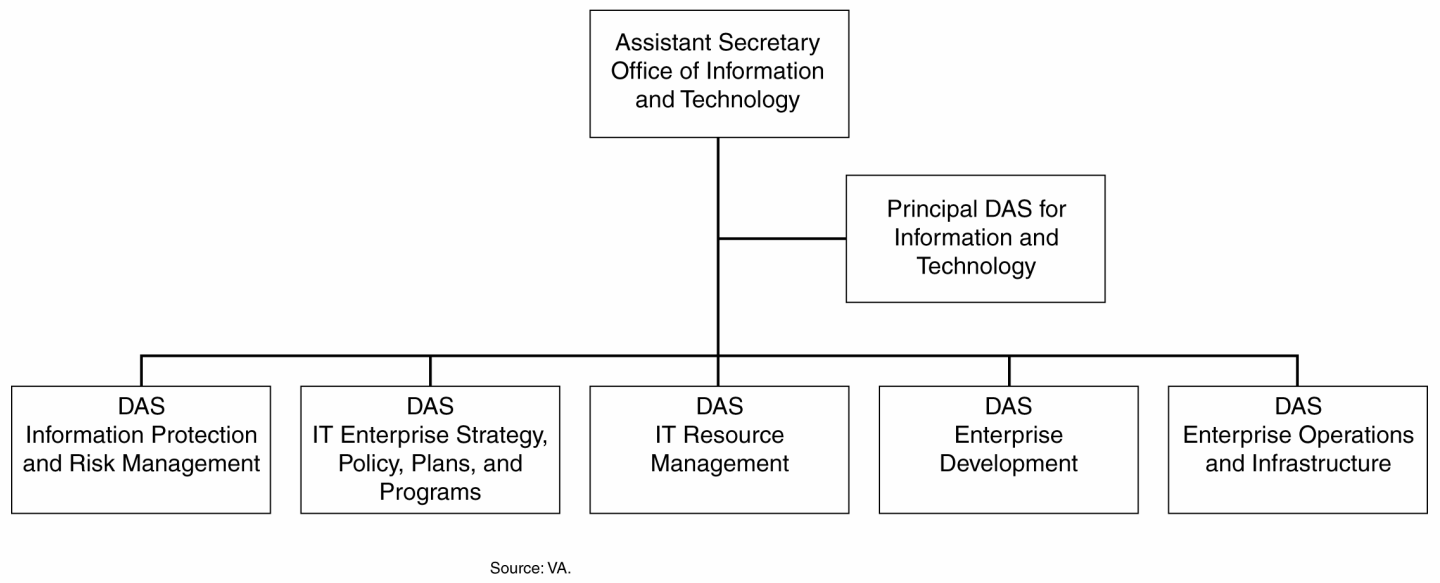
Centralized IT Organization

In response to the challenges that we and others have noted, the department officially began its effort to provide the CIO with greater authority over IT in October 2005. At that time, the Secretary issued an executive decision memorandum granting approval for the development of a new management structure for the department. According to VA, its goals in moving to centralized management are to enable the department to perform better oversight of the standardization, compatibility, and interoperability of systems, as well as to have better overall fiscal discipline for the budget.

In February 2007, the Secretary approved the department's new organizational structure, which includes the Assistant Secretary for Information and Technology, who serves as VA's CIO. As shown in figure 1, the CIO is supported by a principal deputy assistant secretary and five deputy assistant secretaries—new senior leadership positions created to assist the CIO in overseeing functions such as cyber security, IT portfolio management, systems development, and IT operations.

[8]Gartner Consulting, *OneVA IT Organizational Alignment Assessment Project "As-Is" Baseline* (McLean, Virginia; Feb. 18, 2005).

Figure 1: Office of Information and Technology Organizational Chart

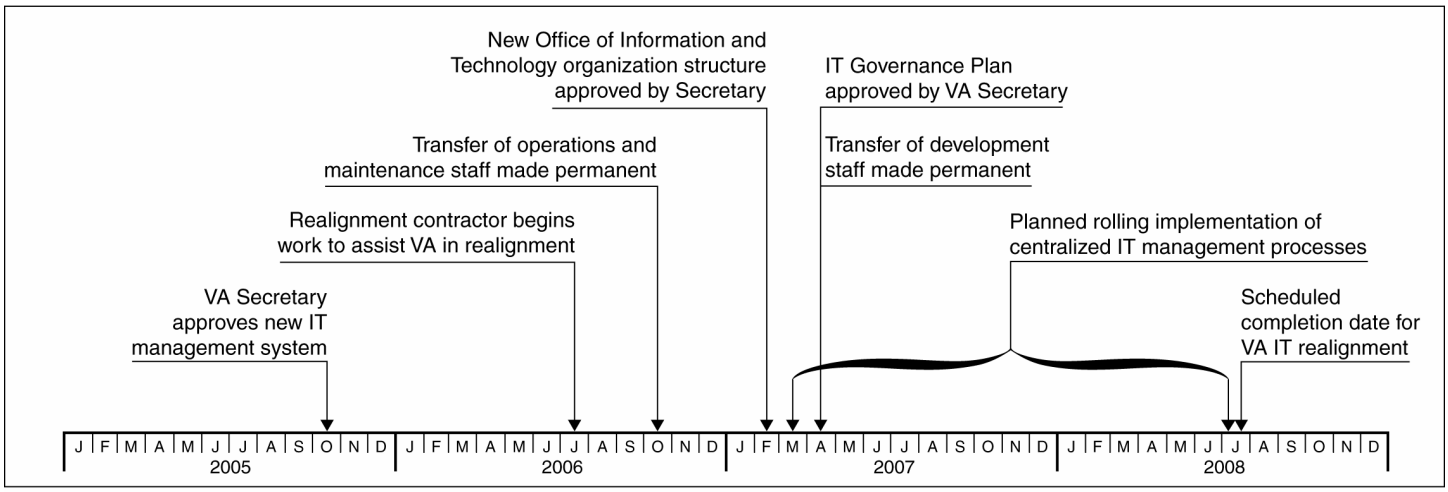


Source: VA.

Note: DAS = Deputy Assistant Secretary

In addition, the Secretary approved an IT governance plan in April 2007 that is intended to enable the Office of Information and Technology to centralize its decision making. The plan describes the relationship between IT governance and departmental governance and the approach the department intends to take to enhance IT governance. The department also made permanent the transfer of its entire IT workforce under the CIO, consisting of approximately 6,000 personnel from the administrations. Figure 2 shows a timeline of the realignment effort.

Figure 2: Timeline of Key Events for VA IT Realignment



Source: GAO analysis of VA data.

Multiple Factors Increasing Risk to Success of Realignment

Although VA has fully addressed two of six critical success factors that we identified as crucial to a major organizational transformation such as the realignment, it has not fully addressed the other four factors, and it has not kept to its scheduled timelines for implementing new management processes that are the foundation of the realignment. Consequently, the department is in danger of not being able to meet its target of completing the realignment in July 2008. In addition, although it has prioritized its implementation of the new management processes, none has yet been implemented. In our recent report,[9] we made six recommendations to ensure that VA's realignment is successfully accomplished; the department generally concurred with our recommendations and stated that it had actions planned to address them.

[9]GAO-07-844.

VA Has Not Fully Addressed All Critical Success Factors

We have identified critical factors that organizations need to address in order to successfully transform an organization to be more results oriented, customer focused, and collaborative in nature.[10] Large-scale change management initiatives are not simple endeavors and require the concentrated efforts of both leadership and employees to realize intended synergies and to accomplish new organizational goals. There are a number of key practices that can serve as the basis for federal agencies to transform their cultures in response to governance challenges, such as those that an organization like VA might face when transforming to a centralized IT management structure.

The department has fully addressed two of six critical success factors that we identified (see table 1).

Table 1: Current Status of VA's Actions to Address Critical Success Factors

Critical success factor	Status as of September 2007
Ensuring commitment from top leadership	**Fully addressed:** Secretary Nicholson approved the new organization structure and the transfer of employees.
Establishing a governance structure to manage resources	**Fully addressed:** Secretary Nicholson approved the IT governance plan, and VA established three new IT governance boards that began meeting earlier this year.
Linking IT strategic plan to organization strategic plan	**Partially addressed:** The department has developed a draft IT strategic plan and expects to finalize it in October 2007.
Using workforce strategic management to identify proper roles for all employees	**Partially addressed:** VA has identified job requirements, has begun to develop career paths for IT staff, and has not yet established a knowledge and skills inventory.
Communicating change to all stakeholders	**Partially addressed:** VA increased communication on the realignment, but has not staffed a key communication office.
Dedicating an implementation team to manage change	**Not addressed:** The department does not have an implementation team to manage the realignment.

Source: GAO.

[10]GAO, *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, GAO-03-669 (Washington, D.C.: July 2, 2003); and *Highlights of a GAO Forum: Mergers and Transformation: Lessons Learned for a Department of Homeland Security and Other Federal Agencies*, GAO-03-293SP (Washington, D.C.: Nov. 14, 2002).

Ensuring commitment from top leadership. The department has fully addressed this success factor. As described earlier, the Secretary of VA has fully supported the realignment. He approved the department's new organizational structure and provided resources for the realignment effort.

However, the Secretary recently submitted his resignation, indicating that he intended to depart by October 1, 2007. While it is unclear what effect the Secretary's departure will have on the realignment, the impending departure underscores the need for consistent support from top leadership through the implementation of the realignment, to ensure that its success is not at risk in the future.

Establishing a governance structure to manage resources. The department has fully addressed this success factor. The department has established three governance boards, which have begun operation. The VA IT Governance Plan, approved April 2007, states that the establishment and operation of these boards will assist in providing the department with more cost-effective use of IT resources and assets.

The department also has plans to further enhance the governance structure in response to operational experience. The department found that the boards' responsibilities need to be more clearly defined in the IT Governance Plan to avoid overlap. That is, one board (the Business Needs and Investment Board) was involved in the budget formulation for fiscal year 2009, but budget formulation is also the responsibility of the Deputy Assistant Secretary for IT Resource Management, who is not a member of this board. According to the Principal Deputy Assistant Secretary for Information and Technology, the department is planning to update its IT Governance Plan within a year to include more specificity on the role of the governance boards in VA's budget formulation process. Such an update could further improve the structure's effectiveness.

Linking IT strategic plan to organization strategic plan. The department has partially addressed this success factor. VA has drafted an IT Strategic Plan that provides a course of action for the

Office of Information and Technology over 5 years and addresses how IT will contribute to the department's strategic plan. According to the Deputy Director of the Quality and Performance Office, the draft IT strategic plan should be formally approved in October 2007. Finalizing the plan is essential to helping ensure that leadership understands the link between VA's organizational direction and how IT is aligned to meet its goals.

Using workforce strategic management to identify proper roles for all employees. The department has partially addressed this success factor. The department has begun to identify job requirements, design career paths, and determine recommended training for the staff that were transferred as part of the realignment. According to a VA official, the department identified 21 specialized job activities, such as applications software and end user support, and has defined competency and proficiency targets[11] for 6 of these activities. Also, by November 2007, VA expects to have identified the career paths for approximately 5,000 of the 6,000 staff that have been centralized under the CIO. Along with the development of the competency and proficiency targets, the department has identified recommended training based on grade level. However, the department has not yet established a knowledge and skills inventory to determine what skills are available in order to match roles with qualifications for all employees within the new organization. It is crucial that the department take the remaining steps to fully address this critical success factor, so that the staff transferred to the Office of Information and Technology are placed in positions that best suit their knowledge and skills, and the organization has the personnel resources capable of developing and delivering the services required.

Communicating change to all stakeholders. The department has partially addressed this success factor. The department began publishing a bimonthly newsletter in June to better communicate with all staff about Office of Information and Technology activities,

[11]Competency refers to required capabilities for performing specialized job activities, such as business process reengineering or database administration. Proficiency targets indicate the level at which the individual can perform these activities.

including the realignment. However, the department has not yet fully staffed the Business Relationship Management Office or identified its leadership. This office is to serve as the single point of contact between the Office of Information and Technology and the administrations; in this role, it provides the means for the Office of Information and Technology to understand customer requirements, promote services to customers, and monitor the quality of the delivered services. A fully staffed and properly led Business Relationship Management Office is important to ensure effective communication between the Office of Information and Technology and the administrations.

Communicating the changed roles and responsibilities of the central IT organization versus the administrations is one of the important functions of the Business Relationship Management Office. These changes are crucial to software development, among other things. Before the centralization of the management structure, each of the administrations was responsible for its own software development. For example, the department's health information system—the Veterans Health Information System and Technology Architecture (VistA)—was developed in a decentralized environment. The developers and the doctors, closely collaborating at local facilities, developed and adapted this system for their own specific clinic needs. The result of their efforts is an electronic medical record that has been fully embraced by the physicians and nurses. However, the decentralized approach has also resulted in each site running a stand-alone version of VistA[12] that is costly to maintain; in addition, data at the sites are not standardized, which impedes the ability to exchange computable information.[13]

Under the new organization structure, approval of development changes for VistA will be centralized at the Veterans Health

[12]VA has achieved an integrated medical information system through the use of the Computerized Patient Record System in VistA, where authorized users are able to access patient health care data from any VA medical facility.

[13]Computable data are in a format that a computer application can act on, for example, to provide alerts to clinicians (of such things as drug allergies) or to plot graphs of changes in vital signs such as blood pressure. VA has standardized its pharmacy and allergy data in its health data repository.

Administration headquarters and then approved for development and implementation by the Office of Information and Technology. The communications role of the Business Relationship Management Office is thus an important part of the processes needed to ensure that users' requirements will be addressed in system development.

Dedicating an implementation team to manage change. The department has not addressed this success factor. A dedicated implementation team that is responsible for the day-to-day management of a major change initiative is critical to ensure that the project receives the focused, full-time attention needed to be sustained and successful.[14] VA has not identified such an implementation team to manage the realignment. Rather, the department is currently managing the realignment through two organizations: the Process Improvement Office under the Quality and Performance Office (which will lead process improvements) and the Organizational Management Office (which will advise and assist the CIO during the final transformation to a centralized structure). However, the Executive Director of the Organizational Management Office[15] has recently resigned his position, leaving one of the two responsible offices without leadership.

In our view, having a dedicated implementation team to manage major change initiatives is crucial to successful implementation of the realignment. An implementation team can assist in tracking implementation goals and identifying performance shortfalls or schedule slippages. The team could also provide continuity and consistency in the face of any uncertainty that could potentially result from the Secretary's resignation.

Accordingly, in our recent report we recommended that the department dedicate an implementation team to be responsible for change management throughout the transformation and that it establish a schedule for the implementation of the management processes.

[14]GAO-07-844.

[15]This official was previously the Director of the IT Realignment Office.

Department Is behind Schedule in Implementing IT Management Processes

As the foundation for its realignment, VA plans to implement 36 management processes in five key areas: enterprise management, business management, business application management, infrastructure, and service support. These processes, which address all aspects of IT management, were recommended by the department's realignment contractor and are based on industry best practices.[16] According to the contractor, they are a key component of the realignment effort as the Office of Information and Technology moves to a process-based organization. Additionally, the contractor noted that with a system of defined processes, the Office of Information and Technology could quickly and accurately change the way IT supports the department.

The department had planned to begin implementing the 36 management processes in March 2007; however, as of early May 2007, it had only begun pilot testing two of these processes.[17] The Deputy Director of the Quality and Performance Office reported that the initial implementation of the first two processes will begin in the second quarter of 2008.

The Principal Deputy Assistant Secretary for Information and Technology acknowledged that the department is behind schedule for implementing the processes, but it has prioritized the processes and plans to implement them in three groups, in order of priority (see attachment 1 for a description of the processes and their implementation priority). According to the Deputy Director of the Quality and Performance Office, the approach and schedule for process implementation is currently under review. Work on the 10 processes associated with the first group is under way, and implementation plans and time frames are being revised. This official told us that initial planning meetings have occurred and

[16]Specifically, these processes are derived from the IT Governance Institute's *Control Objectives for Information and related Technology (CobiT®)* and *Information Technology Infrastructure Library (ITIL)* as configured by the *Process Reference Model for IT (PRM-IT)* from a VA contractor.

[17]These are the risk management and solution test and acceptance processes.

primary points of contact have been designated for the financial management and portfolio management processes, which are to be implemented as part of the first group. The department also noted that it will work to meet its target date of July 2008 for the realignment, but that all of the processes may not be fully implemented at that time.

According to the Principal Deputy Assistant Secretary for Information and Technology, the department has fallen behind schedule with process implementation for two reasons:

- The department underestimated the amount of work required to redefine the 36 process areas. Process charters for each of the processes were developed by a VA contractor and provide an outline for operation under the new management structure. Based on its initial review, the department found that the processes are complicated and multilayered, involving multiple organizations. In addition, the contractor provided process charters and descriptions based on a commercial, for-profit business model, and so the department must readjust them to reflect how VA conducts business.

- With the exception of IT operations, the Veterans Health Administration operates in a decentralized manner. For example, the budget and spending for the medical centers are under the control of the medical center directors. In addition, the Office of Information and Technology only has ownership over about 30 percent of all activities within the financial management process. For example some elements within this process area (such as tracking and reporting on expenditures) are the responsibility of the department's Office of Management;[18] this office is accountable for VA's entire budget, including IT dollars. Thus, the Office of Information and Technology has no authority to direct the Office of Management to take particular actions to improve specific financial management activities.

[18]The Assistant Secretary for Management, who leads the Office of Management, is the department's Chief Financial Officer.

The department faces the additional obstacle that it has not yet staffed crucial leadership positions that are vital to the implementation of the management processes. As part of the new organizational structure, the department identified 25 offices whose leaders will report to the five deputy assistant secretaries and are responsible for carrying out the new management processes in daily operations. However, as of early September, 7 of the leadership positions for these 25 offices were vacant, and 4 were filled in an acting capacity. According to the Principal Deputy Assistant Secretary for Information and Technology, hiring personnel for senior leadership positions has been more difficult than anticipated. With these leadership positions remaining vacant, the department will face increased difficulties in supporting and sustaining the realignment through to its completion.

Until the improved processes have been implemented, IT programs and initiatives will continue to be managed under previously established processes that have resulted in persistent management challenges. Without the standardization that would result from the implementation of the processes, the department risks cost overruns and schedule slippages for current initiatives, such as VistA modernization, for which about $682 million has been expended through fiscal year 2006.

VA Has Much Work Remaining to Resolve Long-Standing Security Weaknesses

Recognizing the importance of securing federal systems and data, Congress passed the Federal Information Security Management Act (FISMA)[19] in December 2002, which sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Using a risk-based approach to information security management, the act requires each agency to develop, document,

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

and implement an agencywide information security program for the data and systems that support the operations and assets of the agency. According to FISMA, the head of each agency has responsibility for delegating to the agency 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).

The May 2006 theft from the home of a VA employee of a computer and external hard drive (which contained personally identifiable information on approximately 26.5 million veterans and U.S. military personnel) prompted Congress to pass the Veterans Benefits, Health Care, and Information Technology Act of 2006.[20] 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 personally identifiable information. In the event of a security incident involving personally identifiable information, VA is required to conduct a risk analysis, and on the basis of the potential for compromise of personally identifiable 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 personally identifiable information.

In a report released last week,[21] we stated that although VA has made progress in addressing security weaknesses, it has not yet fully implemented key recommendations to strengthen its information security practices. It has not implemented two of our four previous recommendations and 20 of 22 recommendations made by the department's inspector general. Among the

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

[21]GAO-07-1019.

recommendations not implemented are our recommendation that it complete a comprehensive security management program and inspector general recommendations to appropriately restrict access to data, networks, and VA facilities; ensure that only authorized changes are made to computer programs; and strengthen critical infrastructure planning to ensure that information security requirements are addressed. Because these recommendations have not yet been implemented, unnecessary risk exists that personally identifiable information of veterans and other individuals, such as medical providers, will be exposed to data tampering, fraud, and inappropriate disclosure.

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 (see table 2). These 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 (mentioned earlier) and the theft of equipment from department facilities, millions of people had their personal information compromised.

Table 2: Number of Incidents by Type Reported to VA's Network and Security Operations Center 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 in 2006 reflects a heightened awareness on the part of VA employees 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.

Since the May 2006 security incident, VA has begun or has continued several major initiatives to strengthen information security practices and secure personally identifiable information within the department. These initiatives include the realignment of its IT management structure, as discussed earlier. Under the realignment, the management structure for information security has changed. In the new organization, the responsibility for managing the program lies with the CISO/Director of Cyber Security (the CISO position has been vacant since June 2006, with the CIO acting in this capacity), while the responsibility for implementing the program lies with the Director of Field Operations and Security. Thus, responsibility for information security functions within the department is divided.

VA officials indicated that the heads of the two organizations are communicating about the department's implementation of security policies and procedures, but 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 these activities are key security management practices. Without a documented process, policies or procedures could be inconsistently implemented throughout the department, which could prevent the CISO from effectively ensuring 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. Developing and documenting these policies and procedures are essential for achieving an improved and effective security management process under the new centralized management model.

In addition to the realignment initiative, the department also has others under way to address security weaknesses. These include developing an action plan to correct identified weaknesses;

establishing an information protection program; improving its incident management capability; and establishing an office to be responsible for oversight of IT within the department. However, implementation shortcomings limit the effectiveness of these initiatives. For example:

- VA's action plan has task owners assigned and is updated biweekly, but department officials have not ensured that adequate progress has been made to resolve items in the plan. Specifically, VA has extended the completion date at least once for 38 percent of the plan items, and it did not have a process in place to validate the closure of the items. In addition, although numerous items in the plan were to develop or revise a policy or procedure, 87 percent of these items did not have a corresponding task with an established timeframe for implementation.

- VA installed encryption software on laptops at facilities inconsistently; however, VA's directive on encryption did not address the encryption of laptops that were categorized as medical devices, which make up a significant portion of the population of laptops at Veterans Health Administration facilities. In addition, the department has not yet fully implemented the acquisition of software tools across the department.

- VA has improved its incident management capability since May 2006 by realigning and consolidating two incident management centers, and made a notable improvement in its notification of major security incidents to US-CERT (the U.S. Computer Emergency Readiness Team), the Secretary, and Congress, but the time it took to send notification letters to individuals was increased for some incidents because VA did not have adequate procedures for coordinating incident response and mitigation activities with other agencies and obtaining up-to-date contact information.

- VA established the Office of IT Oversight and Compliance to conduct assessments of its facilities to determine the adequacy of internal controls and investigate compliance with laws, policies, and directives and ensure that proper safeguards are maintained; however, the office lacked a process 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 use, disclosure, disruption, or loss.

In our report released last week, we made 17 recommendations to assist the department in improving its ability to protect its information and systems. These recommendations included that VA document clearly define coordination responsibilities for the Director of Field Operations and Security and the Director of Cyber Security and develop and implement a process for these officials to coordinate on the implementation of IT security policies and procedures throughout the department. We also made recommendations to improve the department's ability to protect its information and systems, including the development of various processes and procedures to ensure that tasks in the department's security action plans have time frames for implementation.

In summary, effectively instituting a realignment of the Office of Information and Technology is essential to ensuring that VA's IT programs achieve their objectives and that the department has a solid and sustainable approach to managing its IT investments. VA continues to work on improving such programs as information security and systems development. Yet we continue to see management weaknesses in these programs and initiatives (many of a long-standing nature), which are the very weaknesses that VA aims to alleviate with its reorganized management structure. Until the department fully addresses the critical success factors that we identified and carries out its plans to establish a comprehensive set of improved management processes, the impact of this vital undertaking will be diminished. Further, the department may not achieve a solid and sustainable foundation for its new IT management structure.

Mr. Chairman and members of the committee, this concludes our statement. We would be happy to respond to any questions that you may have at this time.

Contacts and Acknowledgements

For more information about this testimony, please contact Valerie C. Melvin at (202) 512-6304 or Gregory C. Wilshusen at (202) 512-6244 or by e-mail at melvinv@gao.gov or wilshuseng@gao.gov. Key contributors to this testimony were made by Barbara Oliver, Assistant Director; Charles Vrabel, Assistant Director; Barbara Collier, Nancy Glover, Valerie Hopkins, Scott Pettis, J. Michael Resser, and Eric Trout.

Attachment 1. Key IT Management Processes to Be Addressed in VA Realignment

In the following table, the priority group number reflects the order in which the department plans to implement each group of processes, with 1 being the first priority group.

Key area	IT management process	Implementation priority group	Description
Enterprise management	IT strategy	2	Addresses long- and short-term objectives, business direction, and their impact on IT, the IT culture, communications, information, people, processes, technology, development, and partnerships
	IT management	2	Defines a structure of relationships and processes to direct and control the IT endeavor
	Risk management	See note a	Identifies potential events that may affect the organization and manages risk to be within acceptable levels so that reasonable assurance is provided regarding the achievement of organization objectives
	Architecture management	2	Creates, maintains, promotes, and governs the use of IT architecture models and standards across and within the change programs of an organization
	Portfolio management	1	Assesses all applications, services, and IT projects that consume resources in order to understand their value to the IT organization
	Security management	2	Manages the department's information security program, as mandated by the Federal Information Security Management Act (FISMA) of 2002
	IT research and innovation	3	Generates ideas, evaluates and selects ideas, develops and implements innovations, and continuously recognizes innovators and learning from the experience
	Project management	1	Plans, organizes, monitors, and controls all aspects of a project in a continuous process so that it achieves its objectives
Business management	Stakeholder requirements management	1	Manages and prioritizes all requests for additional and new technology solutions arising from a customer's needs
	Customer satisfaction management	3	Determines whether and how well customers are satisfied with the services, solutions, and offerings from the providers of IT
	Financial management	1	Provides sound stewardship of the monetary resources of the organization
	Service pricing and contract administration	3	Establishes a pricing mechanism for the IT organization to sell its services to internal or external customers and to administer the contracts associated with the selling of those services
	Service marketing and sales	3	Enables the IT organization to understand the marketplace it serves, to identify customers, to "market" to these customers, to generate "marketing" plans for IT services and support the "selling" of IT services to internal customers

Key area	IT management process	Implementation priority group	Description
	Compliance management	2	Ensures adherence with laws and regulations, internal policies and procedures, and stakeholder commitments
	Asset management	1	Maintains information regarding technology assets, including leased and purchased assets, licenses, and inventory
	Workforce management	2	Enables an organization to provide the optimal mix of staffing (resources and skills) needed to provide the agreed-on IT services at the agreed-on service levels
	Service-level management	2	Manages service-level agreements and performs the ongoing review of service achievements to ensure that the required and cost-justifiable service quality is maintained and gradually improved
	IT service continuity management	1	Ensures that agreed-on IT services continue to support business requirements in the event of a disruption to the business
	Supplier relationship management	3	Develops and exercises working relationships between the IT organization and suppliers in order to make available the external services and products that are required to support IT service commitments to customers
	Knowledge management	3	Promotes an integrated approach to identifying, capturing, evaluating, categorizing, retrieving, and sharing all of an organization's information assets
Business application management	Solution requirements	2	Translates provided customer (business) requirements and IT stakeholder-generated requirements/constraints into solution-specific terms, within the context of a defined solution project or program
	Solution analysis and design	1	Creates a documented design from agreed-on solution requirements that describes the behavior of solution elements, the acceptance criteria, and agreed-to measurements
	Solution build	3	Brings together all the elements specified by a solution design via customization, configuration, and integration of created or acquired solution components
	Solution test and acceptance	See note a	Validates that the solution components and integrated solutions conform to design specifications and requirements before deployment
Infrastructure	Service execution	2	Addresses the delivery of operational services to IT customers by matching resources to commitments and employing the IT infrastructure to conduct IT operations
	Data and storage management	3	Ensures that all data required for providing and supporting operational service are available for use and that all data storage facilities can handle normal, expected fluctuations in data volumes and other parameters within their designed tolerances.
	Event management	3	Identifies and prioritizes infrastructure, service, business and security events, and establishes the appropriate response to those events.
	Availability management	3	Plans, measures, monitors, and continuously strives to improve the availability of the IT infrastructure and supporting organization to ensure that agreed-on requirements are consistently met
	Capacity management	3	Matches the capacity of the IT services and infrastructure to the current and future identified needs of the business
	Facility management	1	Creates and maintains a physical environment that houses IT resources and optimizes the capabilities and costs of that environment
Service support	Change management	1	Manages the life cycle of a change request and activities that measure the effectiveness of the process and provides for its continued enhancement

Key area	IT management process	Implementation priority group	Description
	Release management	1	Controls the introduction of releases (that is, changes to hardware and software) into the IT production environment through a strategy that minimizes the risk associated with the changes
	Configuration management	1	Identifies, controls, maintains, and verifies the versions of configuration items and their relationships in a logical model of the infrastructure and services
	User contact management	3	Manages each user interaction with the provider of IT service throughout its life cycle
	Incident management	2	Restores a service affected by any event that is not part of the standard operation of a service that causes or could cause an interruption to or a reduction in the quality of that service
	Problem management	2	Resolves problems affecting the IT service, both reactively and proactively

Source: GAO.

[a]The department indicated that this process had completed a pilot, but did not assign it to a priority group.

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 "E-mail 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, DC 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, DC 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, DC 20548