United States Government Accountability Office

GAO

Testimony

Before the Senate Committee on Veterans' Affairs

For Release on Delivery
Expected at 9:30 a.m. EDT
Wednesday, September 19, 2007

VETERANS AFFAIRS

Progress Made in Centralizing Information Technology Management, but Challenges Persist

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

GAO
Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-07-1246T, a testimony before the Senate Committee on Veterans' Affairs

September 19, 2007

VETERANS AFFAIRS

Progress Made in Centralizing Information Technology Management, but Challenges Persist

Why GAO Did This Study

The Department of Veterans Affairs (VA) depends on information technology (IT) to effectively serve our nation's veterans, with an IT budget of about $1 billion annually. However, it has encountered numerous challenges in managing its IT programs and initiatives. To address these challenges, VA is realigning its IT organization and management to a centralized model founded on a defined set of improved management processes. Begun in October 2005, the realignment is planned to be complete by July 2008.

In this testimony, GAO discusses its recent reporting on VA's realignment effort and its management of other IT programs and initiatives, including ongoing systems development efforts and work to share electronic health information with the Department of Defense (DOD). To prepare this testimony, GAO reviewed its past work in these areas.

What GAO Recommends

In the reports covered by this testimony, GAO made recommendations aimed at improving VA's management of its IT programs and initiatives.

To view the full product, including the scope and methodology, click on GAO-07-1246T. For more information, contact Valerie Melvin at (202) 512-6304 or melvinv@gao.gov.

What GAO Found

VA has made progress in moving to a centralized management structure for IT; however, at the time of GAO's review in May 2007, the department had still to address certain critical success factors for transformation, and it had not yet institutionalized key IT management processes. VA's plans for realigning the management of its IT program include elements of several of the six factors that GAO identified as critical for the department's implementation of a centralized management structure, and it had fully addressed one factor—ensuring commitment from top leadership—having obtained the Secretary's approval of the realignment and the new IT governance structure. However, as of May 2007, the department did not plan to address one of the critical success factors: dedicating an implementation team to manage change. Having such a team is important, since the implementation of the realignment is expected to continue until July 2008. Without a dedicated team, it is less likely that the implementation will be managed effectively. In addition, although the department had begun to take action to establish improved management processes—a cornerstone of the realignment—it had not made significant progress. As of May 2007, it had begun pilot testing 2 of 36 planned new processes. Until it institutionalizes key processes throughout the department, the full benefits of the realignment may not be realized.

At the same time that it is implementing the realignment, VA is managing ongoing IT programs such as information security and inventory control, and it is continuing initiatives to develop IT systems. The department is managing these programs and initiatives using existing management processes, many of which display the long-standing weaknesses that VA aims to alleviate through its realignment. Some progress has been made: for example, the department took actions to improve controls over IT equipment, such as issuing several new policies to establish guidance and controls for information security, but because the realignment was not yet fully implemented, improved processes for inventory control had not been established. In addition, progress on the development of a modernized compensation and benefits system occurred after the project implemented improved management processes, which the department now plans to apply to all its IT projects. VA also achieved a milestone in the long-term effort to share electronic health information with DOD, having begun to exchange limited medical data with DOD (at selected sites) through an interface between the data repositories for the modern health information systems that each department is developing. To achieve their long-term vision, VA and DOD have much work still to do (such as extending the current capability throughout both departments), and the two departments have not yet projected a final completion date for the whole initiative. Further progress in VA's IT programs and initiatives could be significantly aided by the improved processes that are the cornerstone of the realignment. Until these are fully implemented, the impact of the realignment on these programs and initiatives is uncertain.

Mr. Chairman and Members of the Committee:

I am pleased to participate in today's hearing on the information technology program of the Department of Veterans Affairs (VA). As you know, the department depends on information technology (IT) to effectively serve our nation's veterans, with an IT budget that amounts to about $1 billion annually. However, VA has encountered numerous challenges in managing its IT resources, as we have reported over the years. In our more recent reporting, we have identified challenges in security management, inventory control, project management, and other IT management processes.[1] One factor contributing to the development of these challenges has been the department's management structure,[2] which until recently was decentralized and gave the VA administrations[3] and headquarters offices[4] 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. The goals of the realignment were to centralize IT management under the department-level Chief Information Officer (CIO) and to standardize operations and development of systems across the department through the use of new management processes based on

[1] For example, 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); *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); *Veterans Affairs: Lack of Accountability and Control Weaknesses over IT Equipment at Selected VA Locations*, GAO-07-1100T (Washington, D.C.: July 24, 2007); and *Veterans Benefits Administration: Progress Made in Long-Term Effort to Replace Benefits Payment System, but Challenges Persist*, GAO-07-614 (Washington, D.C.: Apr. 27, 2007).

[2] GAO, *Veterans Affairs: The Role of the Chief Information Officer in Effectively Managing Information Technology*, GAO-06-201T (Washington, D.C.: Oct. 20, 2005*)*; and *Veterans Affairs: The Critical Role of the Chief Information Officer Position in Effective Information Technology Management*, GAO-05-1017T (Washington, D.C.: Sept. 14, 2005).

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

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

industry best practices. Completion of the realignment is scheduled for July 2008.

At your request, my testimony today will summarize our work on the department's efforts in moving to a centralized IT management model, which will affect all of VA's IT programs and initiatives. In this context, we will also discuss our recent work on

- information security,
- inventory control over IT equipment,
- migrating existing ("legacy") benefits systems to modern platforms, and
- sharing electronic health information with the Department of Defense (DOD) and the prognosis for a DOD/VA bidirectional interoperable electronic health record.

In developing this testimony, we reviewed our previous work in these areas. All work covered in this testimony was performed in accordance with generally accepted government auditing standards.

Results in Brief

VA has made progress in moving to a centralized management structure for IT; however, at the time of our review in May 2007, it had still to address some critical success factors for transformation, and it had not yet institutionalized key IT management processes.[5] The department's plans for realigning the management of its IT program include elements of several of the six factors that we identified as critical for its implementation of a centralized management structure. However, as of May 2007, VA did not plan to address one of the critical success factors: dedicating an

[5] 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).

implementation team to manage change. Having such a team is important at this stage, because the realignment is not expected to be completed until July 2008. Without a team dedicated to managing the realignment, it is less likely that the department will be able to ensure that the realignment is managed effectively throughout its implementation. In addition, although the department had begun to take action to establish improved IT management processes—a cornerstone of the realignment—it had not made significant progress at the time of our report. As of May 2007, it had begun pilot testing 2 of 36 planned new processes. Until it institutionalizes key management processes throughout the department, the full benefits of the realignment may not be realized.

In the meantime, VA is undertaking a number of programs and initiatives that depend on the effective management and use of IT resources. The department has made progress in its programs and initiatives, but much work remains.

- In a September 2007 report, we state that although VA has made progress in addressing security weaknesses, it has not yet fully implemented key recommendations to strengthen its information security practices.[6] In addition, 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.
- With regard to the department's IT inventory control, we reported recently that a weak overall control environment for IT equipment at four audited locations posed a significant security vulnerability to the nation's veterans with regard to sensitive data maintained on

[6] 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).

this equipment.[7] VA had taken some actions to improve controls over IT equipment, such as issuing several new policies to establish guidance and controls for information security. In addition, the organizational realignment had begun, but as it was not yet fully implemented, improved processes for inventory control had not been established.

- VBA has been pursuing efforts to migrate benefits processing from its aging legacy system and develop modernized replacement systems.[8] We reported that two initiatives (one on compensation and pension payments and another on education benefits) had both been hindered by project management weaknesses and in particular the lack of integrated project plans. In April 2007, we reported that the compensation and pension replacement project had improved its management processes and made progress; VA concurred with our recommendation that the improved processes be incorporated into specific policy and guidance for all IT projects in the department. Such processes could benefit the education benefits project: when we reported in July 2007, the initiative had achieved some enhancements in claims processing, but the absence of an integrated project plan meant that critical elements were missing for effectively guiding the project to completion, such as an overall approach for coordinating various improvement initiatives.

- As we testified in May 2007, VA and DOD have made progress in both long- and short-term initiatives to share health information, but much work remains to achieve the goal of a shared electronic

[7] 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).

[8] GAO, *Veterans Benefits Administration: Progress Made in Long-Term Effort to Replace Benefits Payment System, but Challenges Persist*, GAO-07-614 (Washington, D.C.: Apr. 27, 2007), and *Veterans Affairs: Improved Planning Needed to Guide Development and Implementation of Education Benefits System*, GAO-07-1045 (Washington, D.C.: July 31, 2007).

medical record and seamless transition between the two departments.[9]

- Under their long-term initiative, the departments had begun to exchange limited medical data (at selected sites) through an interface between the data repositories for the modern health information systems that each department is developing. Although implementing this interface is a milestone toward the departments' long-term goal, VA and DOD must still extend the current capability throughout both departments, finish developing their two modernized systems, and transition from their existing systems.[10] The departments have not yet projected a final completion date for the whole initiative.
- In their near-term efforts, the departments have completed a system for one-way transfer of health information from DOD to VA when service members leave the military, and they are conducting demonstration projects to exchange limited data at selected sites. The departments have also established ad hoc processes (such as scanning paper records) to meet the immediate need to provide data on severely wounded service members to VA's polytrauma centers.

These multiple initiatives and ad hoc processes highlight the need for a project plan that integrates both long- and short-term initiatives. Without such a plan, it remains unclear how all the initiatives are to be incorporated into an overall strategy focused on achieving the departments' goal of comprehensive, seamless exchange of health information.

In the reports covered by this testimony, we have made numerous recommendations aimed at improving the department's

[9] GAO, *Information Technology: VA and DOD Are Making Progress in Sharing Medical Information, but Are Far from Comprehensive Electronic Medical Records*, GAO-07-852T (Washington, D.C.: May 8, 2007).

[10] Among other tasks required to complete development, the two departments must agree to standards and populate the data repositories for the categories of medical information that have not yet been addressed: that is, all categories except outpatient pharmacy and drug allergy data.

management of its IT programs and initiatives. VA has agreed with these recommendations and has taken action or plans to take action to implement them. If this implementation is properly executed, it could help the department to realize the expected benefits of the realignment, as well as the aims of its programs and initiatives.

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. Its three major components, the Veterans Benefits Administration (VBA), the Veterans Health Administration (VHA), and the National Cemetery Administration, are primarily responsible for carrying out this mission. 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 providing access to medical information to ensure high-quality health care 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 achieving its vision of creating "One VA"—that is, integrating IT resources to enable department employees to help veterans obtain services and information more quickly and effectively. One major challenge was that the department's information systems and services were highly decentralized and that its administrations controlled a majority of the IT budget.[11] As we have previously pointed out, it is crucial for the department CIO to ensure that well-established and integrated processes for leading, managing, and controlling investments are

[11] 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.

followed throughout the department. Similarly, a contractor's assessment of VA's IT organizational alignment, issued in February 2005, noted the lack of control over how and when money is spent.[12] The assessment found that project managers within the administrations had the ability to shift money to support individual projects. Also, according to the assessment, 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.

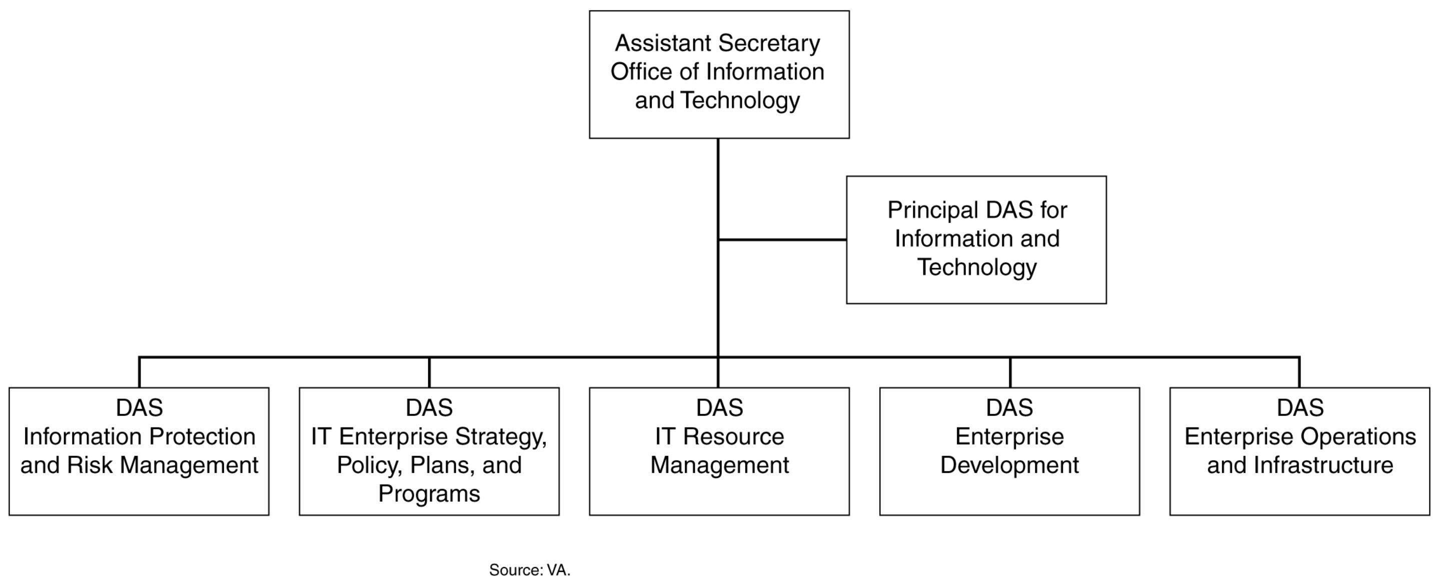
VA Is Transforming its IT Organization to a Centralized Model

In response to the challenges that we and others 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 IT management structure for the department. According to VA, its goals in moving to centralized management are to provide the department better oversight over the standardization, compatibility, and interoperability of IT systems, as well as better overall fiscal discipline for the budget. By July 2006, the department's realignment contractor began work to assist with the realignment effort.

In February 2007, the Secretary approved the department's new organization 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.

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

Figure 1: Organizational Chart for VA Office of Information and Technology



Source: VA.

Note: DAS = Deputy Assistant Secretary.

In April 2007, the Secretary approved a governance plan 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 governance.

VA's Realignment Depends on Establishing Standardized IT Management Processes

As the foundation for its realignment, VA plans to implement improved management processes in five key areas: enterprise management, business management, business application management, infrastructure, and service support. The particular management processes, recommended by the department's realignment contractor, were based on industry best practices[13] and encompass all areas of IT management, such as those necessary for

[13] 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.

effective IT programs (such as security management and asset management processes) and IT initiatives (such as risk management and project management processes). In attachment 1, we provide brief descriptions of the 36 IT management processes to be addressed in VA's realignment.

According to the contractor, establishing improved management processes and standardizing these processes across the department are essential to the effectiveness of the centralized management model. By implementing these improved processes, VA expects to correct deficiencies it has encountered as a result of its decentralized management approach. Proper implementation should result in institutionalizing best management practices that will be sustained regardless of future leadership changes at the department. According to the contractor, with a system of defined management processes, the Office of Information and Technology could quickly and accurately change the way IT supports the department. The contractor also noted that failure to include such processes in the realignment would introduce the risk that any progress in completing the realignment would be the result of trial and error.

Successful Organization Transformations Are Based on Critical Success Factors

We have reported in the past[14] on key factors that are needed in order to successfully transform an organization to be more results oriented, customer focused, and collaborative in nature. We reported that 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. We also noted that 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.

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

Among the significant factors we identified as critical for ensuring the success of VA's move to centralized management are

- ensuring commitment from top leadership,
- establishing a governance structure to manage resources,
- linking the IT strategic plan to the organization strategic plan,
- using workforce strategic management to identify proper roles for all employees,
- communicating change to all stakeholders, and
- dedicating an implementation team to manage change.

Successful Implementation of the Realignment Effort Requires Continued Focus on Critical Success Factors and Implementation of Improved Management Processes

In our recent review of the department's effort to realign its IT program, we evaluated, among other things, whether the realignment plan includes the critical factors for successful transformation as discussed above.[15] We reported that VA's realignment plan included elements of several of the six critical success factors that we identified. However, VA had not fully addressed all six factors. Only one factor had been fully addressed; additional work remained on the other five factors, as shown in table 1.

[15] 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).

Table 1: Summary of VA's Actions Addressing Critical Success Factors as of May 2007

Critical success factor	Addressed	Progress
Ensuring commitment from top leadership	Yes	Secretary approved the new IT organization structure and the transfer of employees
Establishing a governance structure to manage resources	Partially	Secretary approved the IT governance plan, but VA has not established IT governance boards or process descriptions for centrally managing IT
Linking IT strategic plan to organization strategic plan	No	VA has not yet updated its IT strategic plan to reflect the new organization, but it has established a date by which it intends to update the plan
Using workforce strategic management to identify proper roles for all employees	Partially	VA has identified workforce management responsibilities, but it has not established a knowledge and skills inventory
Communicating change to all stakeholders	Partially	VA has addressed staff concerns about the realignment through memorandums and conferences, but it has not fully staffed offices that will facilitate communication
Dedicating an implementation team to manage change	No	VA does not plan to establish a realignment implementation team

Source: GAO.

The department had fully addressed the first critical success factor, ensuring commitment from top leadership, as demonstrated by the Secretary's actions in support of the realignment. Besides approving the transfer of personnel to the centralized office, the Secretary approved in February 2007 a new organization structure for centralized IT management.

Since undertaking the realignment, VA concentrated its efforts on transferring approximately 6,000 staff to the CIO's office from the administrations and staff offices and on creating the new centralized organizational structure. As shown in the table, VA had begun or planned to begin actions on four other critical success factors, but it had not completed the actions. For example, the department approved its governance plan to address how the Office of Information and Technology will manage resources; however, it had not yet established the boards that are to provide governance over the centralized structure. In addition, although the department had identified the responsibilities for managing its workforce within its new structure, it had not yet established a knowledge and skills inventory to help determine the proper roles for all employees in the new organization.

VA had neither addressed nor planned to address the last critical success factor: dedicating an implementation team to manage change. Although it had highlighted the importance of managing change in its realignment documentation, VA did not plan to establish a realignment implementation team. As we have pointed out,[16] 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. Specifically, the implementation team is important to ensuring that various change initiatives are implemented in a coherent and integrated way. The team must have the necessary authority and resources to set priorities, make timely decisions, and move quickly to implement the transformation. In addition, the implementation team can assist in tracking implementation goals for a change initiative and identifying performance shortfalls or schedule slippages. It is important for the team to use performance metrics to provide a succinct and concrete statement of expected performance versus actual performance. Because of its close involvement with the change initiative, the implementation team can also suggest corrections to remedy any problems.

The department had not addressed this critical success factor: it had not dedicated an implementation team to manage the realignment effort and track its progress. At the conclusion of our review in June 2007, staff from the IT realignment office, which was responsible for overseeing the realignment, had been reassigned to other areas of responsibility within the department's new structure. In addition, the Director of the Realignment Office told us that multiple offices would assume responsibility for managing the realignment through July 2008: the Office of Quality and Performance Management would oversee process implementation across the Office of

[16] GAO, *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, GAO-03-669 (Washington, D.C.: July 2, 2003).

Information and Technology, and the Office of Oversight and Compliance Management would assess whether the department is complying with the new processes. However, there was no one group responsible for managing the realignment in its entirety. Without such a dedicated group, it is less likely that VA will be able to ensure that the realignment is managed effectively throughout its implementation.

With regard to the new IT management processes, the department had begun to take action, but it had not made significant progress at the time of our report. The department had planned to begin implementing 9 of the 36 new processes in March 2007. However, the department had missed key implementation dates for these processes. As of May 2007, it had begun pilot testing two of the new processes: the risk management process and the solution (that is, business application) test and acceptance process.

Thus, although the department had taken positive steps in moving to centralized IT management, it had much more work to complete before the realignment can be considered finished and a success. If VA does not continue to address the critical success factors we identified and develop and implement the new management processes by their target date, the department may continue to operate in a decentralized manner and risk not fully realizing the long-term benefits of the realignment.

Accordingly, we recommended that the department dedicate an implementation team responsible for change management throughout the transformation and that it develop detailed IT governance process descriptions that identify how IT resources will be managed in the centralized organization. We also made seven additional recommendations aimed at ensuring that the realignment is successfully accomplished. The department generally concurred with our recommendations and stated that it has taken action or has actions under way to address each of our recommendations.

Improved Processes Planned under the Realignment Are Not Yet in Place for IT Programs and Initiatives

Although IT management has been centralized under the CIO, at the time of our review, IT programs and initiatives continued to be managed under previously established processes. The key processes to be used as the foundation for the realignment had not yet had an impact on IT programs (specifically, security and inventory management) or initiatives (such as VBA's modernization efforts and VHA's initiatives on sharing medical data with DOD).

Sustained Management Commitment and Oversight Are Vital to Resolving Long-Standing Security Weaknesses

As mandated by the Federal Information Security Management Act (FISMA) of 2002,[17] every agency is to establish an information security program. In addition, security management is a key management process that under the realignment is to be established uniformly across the department. VA's IT systems contain sensitive information that is vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure.

This vulnerability was highlighted by an incident in May 2006, when VA announced that computer equipment containing personally identifiable information[18] on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. Until the equipment was recovered, veterans did not know whether their information was likely to be misused.

[17] FISMA, Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002). Further, the Veterans Benefits, Health Care, and Information Technology Act of 2006, Pub. L. No. 109-461 (Dec. 22, 2006) contains specific requirements for VA's information security program.

[18] "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 his or her 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.

In a September 2007 report, we state that although VA has made progress in addressing security weaknesses, it has not yet fully implemented key recommendations to strengthen its information security practices.[19] It has implemented 2 of our 4 previous recommendations and only 2 of the 22 recommendations made by the department's inspector general (IG). Among those recommendations not implemented are our recommendation that it complete a comprehensive security management program and an IG recommendation to strengthen critical infrastructure planning to ensure that information security requirements are addressed. Because these recommendations have not yet been implemented, the department will be at increased risk that personal information of veterans and other individuals, such as medical providers, may be exposed to data tampering, fraud, and inappropriate disclosure.

Our report describes several major initiatives that VA has begun or continued since the May 2006 security incident, in efforts to strengthen information security practices and secure personal information within the department. Among these initiatives are the department's efforts to reorganize its management structure to provide better oversight and fiscal discipline over its IT systems.[20]

Establishing 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 chief information security officer (CISO) to assist in carrying out his responsibilities. One mechanism organizations can adopt to achieve effective coordination and communication is to

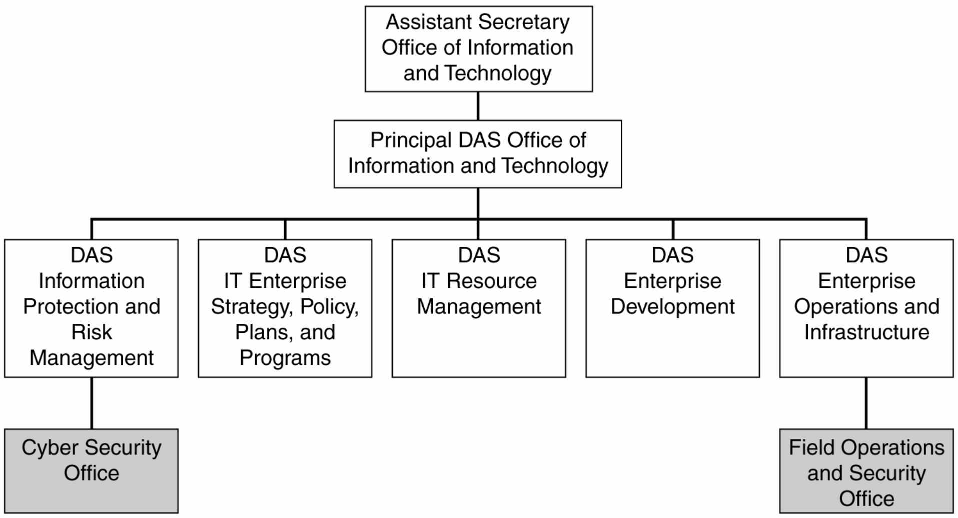
[19] GAO, *Information Security: Sustained Management Commitment and Oversight Are Vital to Resolving Long-standing Weaknesses at the Department of Veterans Affairs*, GAO-07-1019 (Washington, D.C.: Sept. 7, 2007).

[20] Other initiatives are developing a remedial action plan; establishing an information protection program; improving incident management capability; and establishing an office responsible for oversight and compliance of IT within the department.

establish a central security management office or group to coordinate departmentwide security-related activities.[21] To ensure that information security activities are effective across an organization, the management structure should also include clearly defined roles and responsibilities for all security staff and coordination of responsibilities among individual staff.

Under the realignment, the management structure for information security has changed, but improved security management processes have not yet been completely developed and implemented. In particular, under the new structure, responsibility for information security functions within the department is divided between two organizations (see fig. 2), but no documented process yet exists for the two responsible offices to coordinate with each other in managing and implementing the departmentwide security program.

Figure 2: Security Functions in New Office of Information and Technology Structure


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.

[21] 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).

Under the new organization, the Director of the Cyber Security Office (who is also the department's designated CISO)[22] has responsibility for developing and maintaining a departmentwide security program, among other things. However, the Director of the Field Operations and Security Office is responsible for implementing the program. Although VA officials indicated that these officials are communicating about the department's implementation of security policies and procedures, 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. In addition, without a defined process and responsibilities, 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.

Accordingly, among the actions we recommended to the department was to document clearly defined coordination responsibilities for the Director of Field Operations and Security and the Director of Cyber Security, as well as to 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 15 other 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. VA generally agreed with our recommendations

[22] The CISO position is currently unfilled, having been vacant since June 2006. 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.

and stated that it had already implemented some of the recommendations and had actions under way to address the others.

Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation

In light of reported weaknesses in VA inventory controls and reported thefts of laptop computers and data breaches, the adequacy of such controls has been an ongoing concern. In July 2007, we reported and testified on an assessment of the risk of theft, loss, or misappropriation of IT equipment at selected VA medical centers.[23] Our assessment found that a weak overall control environment for IT equipment at the four locations we audited posed a significant security vulnerability to the nation's veterans with regard to sensitive data maintained on this equipment. According to our *Standards for Internal Control in the Federal Government*, agencies are required to establish physical controls to safeguard vulnerable assets, such as IT equipment, which might be vulnerable to risk of loss; in addition, federal records management law requires federal agencies to record essential transactions. However, we reported in July that current VA property management policy does not provide guidance for creating records of inventory transactions as changes occur. Also, policies requiring annual inventories of sensitive items (such as IT equipment), adequate physical security, and immediate reporting of lost and missing items had not been enforced.

Our statistical tests of physical inventory controls at the four locations identified a total of 123 missing IT equipment items, including 53 computers that could have stored sensitive data. The lack of user-level accountability and inaccurate records on status, location, and item descriptions make it difficult to determine the extent to which actual theft, loss, or misappropriation may have

[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).

occurred without detection. Table 2 summarizes the results of our statistical tests at each location.

Table 2: Current IT Inventory Control Failures at Four Test Locations

Control failures	Washington, D.C., medical center	Indianapolis, medical center	San Diego, medical center	VA HQ offices
Missing items	28%	6%	10%	11%
Incorrect user organization	80%	69%	70%	11%
Incorrect location	57%	23%	53%	44%
Recordkeeping errors	5%	0%	5%	3%

Source: GAO analysis.

Note: Each of these estimates has a margin of error, based on a two-sided, 95 percent confidence interval, of ±10 percent or less.

We also found that the four VA locations had reported over 2,400 missing IT equipment items, valued at about $6.4 million, identified during physical inventories performed in fiscal years 2005 and 2006. Missing items were often not reported for several months and, in some cases, several years. It is very difficult to investigate these losses because information on specific events and circumstances at the time of the losses is not known. Further, our limited tests of computer hard drives in the excess property disposal process found hard drives at two of the four case study locations that contained personal information, including veterans' names and Social Security numbers. Our tests did not find any remaining data after sanitization procedures were performed.[24] However, weaknesses in physical security at IT storage locations and delays in completing the data sanitization process heighten the risk of data breach.

Although VA had taken some actions to improve controls over IT equipment (such as issuing several new policies to establish guidance and controls for IT security) and had reorganized and

[24] Sanitization is the process of removing all information from computer media. VA information resource management (IRM) personnel and contractors follow National Institute of Standards and Technology (NIST) Special Publication 800-88 guidelines, as well as more stringent Department of Defense (DOD) policy in DOD 5220.22-M, *National Industrial Security Program Operating Manual*, ch. 8, § 8-301, which requires performing three separate erasures for media sanitization.

centralized the IT function within the department under the CIO, we reported that these actions had not yet been fully implemented. The new CIO organization had no formal responsibility for medical equipment that stored or processed patient data and did not address roles or necessary coordination between information resource management and property management personnel with regard to inventory control of IT equipment. The Assistant Secretary for Information and Technology, who serves as the CIO, told us that the new CIO organization structure will include a unit that will have responsibility for IT equipment asset management once it becomes operational. However, at the time of our report, this unit had not yet been funded or staffed. To ensure accountability and safeguarding of sensitive IT equipment, effective implementation will be key to the success of the department's IT policy and organizational changes.

We made 12 recommendations for actions to be taken by the department to help minimize the risk of loss, theft, and misappropriation of government IT equipment used in VA operations. The recommendations included establishing policies and procedures that require, among other things, recording inventory transactions and establishing specific, individual user-level accountability. VA management generally agreed with our findings and concurred with all 12 recommendations, noting that it had actions planned or under way to address them.

Challenges Persist for Efforts to Migrate from the Aging Benefits Delivery Network

To administer various benefits programs, VBA relies on an aging system, the Benefits Delivery Network (BDN). The BDN, which has been in operation for more than 40 years, is based on antiquated software programs, which have become increasingly difficult and costly to maintain. VBA is in the process of replacing the BDN with a faster, more flexible, and higher capacity system.

Replacing the BDN has been a focus of systems development efforts at VBA since 1986.[25] VBA currently depends on the BDN to administer programs for three types of benefits: (1) compensation and pension, (2) education, and (3) vocational rehabilitation and employment (VRE) services.[26] Originally, the administration planned to modernize the entire system, but after experiencing numerous false starts and spending approximately $300 million on the overall modernization of the BDN, VBA revised its strategy in 1996. First, it narrowed its focus to replacing only those functionalities that support the compensation and pension program, and began developing a replacement system, which it generally refers to as the Veterans Service Network (VETSNET).[27] Then, in December 1999, it began an initiative, The Education Expert System (TEES), to move its education claims processing systems from the BDN to new technology platforms and a new architecture, as a way to improve its education benefits delivery services. (We have not evaluated the VRE program or possible plans to migrate VRE operations from the BDN.)

Progress Made in Long-Term Effort to Replace Benefits Payment System, but Challenges Persist

When VBA began the VETSNET project in 1996, it planned to complete the replacement system in May 1998 at an estimated cost of $8 million. However, over the years, VBA encountered numerous problems in completing the replacement system. We have reported

[25] The BDN currently runs on aging software: COBOL programs and a nonrelational database. Analysts have indicated that moving from a nonrelational database of the BDN type to a more modern relational database is a challenging task.

[26] VBA also provides loan guaranty and life insurance benefits for veterans and their families, but these programs do not depend on the BDN.

[27] It also refers to the initiative as the compensation and pension or C&P replacement system.

on this topic several times, making numerous recommendations.[28] Although VA concurred with our recommendations and took several actions to address them, its actions were not sufficient to implement all our recommendations or establish the program on a solid footing: certain basic requirements of sound project management, such as an integrated project plan for the replacement system, continued to be lacking.

In 2005, because of concerns about continuing problems with the replacement project, VA contracted for an independent assessment of the department's options for the project, including whether the project should be terminated. This assessment, conducted by the Carnegie Mellon Software Engineering Institute (SEI), concluded that the replacement project faced many risks arising from management and organizational issues, but no technical barriers that could not be overcome.[29] According to SEI, a new system was still needed, and VBA would not be able to successfully deliver a full, workable solution unless it addressed its management and organizational weaknesses. SEI recommended that VBA continue to work on the project at a reduced pace, while taking an aggressive approach to addressing the identified weaknesses.

We reported in April 2007[30] that VBA was generally following the course of action recommended by SEI: it was continuing to work on

[28] GAO, *Software Capability Evaluation: VA's Software Development Process Is Immature*, GAO/AIMD-96-90 (Washington, D.C.: June 19, 1996); *Veterans Benefits Modernization: VBA Has Begun to Address Software Development Weaknesses But Work Remains*, GAO/AIMD-97-154 (Washington, D.C.: Sept.15, 1997); *VA Information Technology: Progress Continues Although Vulnerabilities Remain*, GAO/T-AIMD-00-321 (Washington, D.C.: Sept. 21, 2000); *VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist*, GAO-01-550T (Washington, D.C.: Apr. 4, 2001); *VA Information Technology: Management Making Important Progress in Addressing Key Challenges*, GAO-02-1054T (Washington, D. C.: Sept. 26, 2002); and *Information Technology: VA and DOD Face Challenges in Completing Key Efforts*, GAO-06-905T (Washington, D.C.: June 22, 2006).

[29] Kathryn Ambrose, William Novak, Steve Palmquist, Ray Williams, and Carol Woody, Report *of the Independent Technical Assessment on the Department of Veterans Affairs VETSNET Program* (Carnegie Mellon Software Engineering Institute, September 2005).

[30] GAO, *Veterans Benefits Administration: Progress Made in Long-Term Effort to Replace Benefits Payment System, but Challenges Persist*, GAO-07-614 (Washington, D.C.: Apr. 27, 2007).

the replacement initiative at a slower pace, while taking action to address identified weaknesses in overall management and software development processes. For example, VBA established a new governance structure, and it took steps to improve its software development processes, such as establishing risk and requirements management processes. However, some processes had not been addressed, such as capacity planning and management, which will be important for ensuring that further development does not lead to processing slowdowns. Further, VBA had not yet documented policies and procedures to institutionalize all the process improvements that it made on the replacement initiative, having first concentrated its efforts on establishing the governance and building the organization. If VBA does not institutionalize these improvements, it increases the risk that they may not be maintained through the life of the project or be available for application to other development initiatives.

As of April 2007, VBA had developed critical functionalities needed to process and pay certain original compensation claims using the replacement system. According to VBA officials, all five of the major software applications that make up the new system were being used in VA's regional offices to establish and process new compensation claims for veterans. In April 2007, the replacement system was providing monthly compensation payments to almost 50,000 veterans (out of about 3 million veterans who receive such payments). Nonetheless, the system requires further development, and VBA still faces the substantial task of converting records for the approximately 3.5 million beneficiaries on the BDN to the replacement system.

Under the realignment, the responsibility for all system development projects has moved from VBA to the central CIO organization: specifically, the Deputy Assistant Secretary for Enterprise Development. Thus, this official is now responsible for completing the development and implementation of VETSNET. Accordingly, we recommended that the CIO document and incorporate the improved processes for managing risks, requirements, and defects into specific policy and guidance for the replacement initiative and for future use throughout VBA. VA concurred with our recommendation and stated that the VETSNET project management processes will be incorporated into a set of standard project management policies, processes, and procedures for all IT projects in VA. Further, the CIO has identified the VETSNET governance model as the model for all VA enterprisewide IT projects, and it is being implemented in other VA priority IT development programs.

In addition, we made five other recommendations aimed at sustaining the improved management and software development processes currently being used by VETSNET project management, including processes for capacity planning and management. The Secretary also agreed with these recommendations and described actions planned in response.

Improved Planning Needed to Guide Development and Implementation of Education Benefits System

The Education Expert System (or TEES) effort aims to replace the existing education benefits systems on the BDN with a new rules-based system that will add more automated capabilities, eliminate most human intervention, and enable faster and more accurate processing of education claims. When it began the initiative, VBA had planned to complete the new system by September 2005; however, in 2004, the department refocused and rebaselined the system's development effort. VA currently estimates that the TEES initiative will be completed by 2011.

When we reported on this matter in July 2007, VBA had enhanced education benefits claims processing by developing certain functionalities to allow information to be captured in an electronic format.[31] For example, it had developed automated systems that allow (1) education institutions to provide online enrollment certifications, (2) students to provide online and telephonic verification of enrollment, and (3) the public to inquire about approved academic programs, licensing and certification programs, and national exams. However, although VBA had identified other initiatives as necessary to complete the new system and eliminate

[31] GAO, *Veterans Affairs: Improved Planning Needed to Guide Development and Implementation of Education Benefits System*, GAO-07-1045 (Washington, D.C.: July 31, 2007).

most human intervention, it had not taken action on these initiatives, which included moving the processing and payment functionality used for many education claims from the BDN to new technology.

Contributing to our concerns was that VBA did not have an integrated project plan for the TEES initiative. According to agency officials, the plan that had been developed in 2001 has not been updated since 2004, when program goals were modified. Because VBA did not have an integrated project management plan, it lacked critical elements needed to effectively guide the initiative to completion (such as a full description of the scope of the system development efforts) and an overall approach for coordinating its various education claims initiatives (such as the BDN code conversion effort). Without these critical elements, the department would be at risk of wasting millions of dollars on education claims processing initiatives that may overlap or be duplicative.

One reason for this management weakness is the lack of well-defined IT management processes across VA, which is to be addressed by the realignment. Under the realignment, the responsibility for TEES, like other system development projects, has moved from VBA to the Deputy Assistant Secretary for Enterprise Development, who is part of the central CIO organization. At the time of our report, the TEES project had not yet been affected by VA's stated intention of incorporating the VETSNET project management processes into a set of standard project management policies, processes, and procedures for all IT projects in the department. Establishing improved IT management processes is vital to ensuring effective project management and thus the future development and implementation of TEES.

To ensure the successful implementation of TEES, we made three recommendations aimed at ensuring that a comprehensive, integrated project plan to coordinate and manage the initiative would be developed. VA concurred with our recommendations and described actions planned to address them.

VA Is Making Progress in Sharing Medical Information with DOD, but the Two Departments Are Far from Comprehensive Electronic Medical Records

For almost 10 years, VA and DOD have been engaged in multiple efforts to share electronic medical information, which is important in helping to ensure that active-duty military personnel and veterans receive high-quality health care. These include efforts focused on the long-term vision of a single "comprehensive, lifelong medical record for each service member"[32] that would allow a seamless transition between the two departments, as well as more near-term efforts to meet immediate needs to exchange health information, including responding to current military crises.

As we testified in May 2007, VA and DOD have made progress in sharing health information, but much work remains to achieve the goal of a shared electronic medical record and seamless transition between the two departments.[33] In their long-term initiatives, each department is developing its own modern health information system to replace its legacy systems, and they are collaborating on a program to develop an interface to enable these modernized systems to share data and ultimately to have interoperable[34] electronic medical records. Unlike the legacy systems, the modernized systems are to be based on computable data: that is, the data are to be 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. According to the departments, such computable data

[32] In 1996, the Presidential Advisory Committee on Gulf War Veterans' Illnesses reported on many deficiencies in VA's and DOD's data capabilities for handling service members' health information. In November 1997, the President called for the two agencies to start developing a "comprehensive, lifelong medical record for each service member," and in 1998 issued a directive requiring VA and DOD to develop a "computer-based patient record system that will accurately and efficiently exchange information."

[33] GAO, *Information Technology: VA and DOD Are Making Progress in Sharing Medical Information, but Are Far from Comprehensive Electronic Medical Records*, GAO-07-852T (Washington, D.C.: May 8, 2007).

[34] Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

contribute significantly to patient safety and the usefulness of electronic medical records.

At the time of our testimony, the departments had begun to implement the first release of the interface between their modernized data repositories, and computable outpatient pharmacy and drug allergy data were being exchanged at seven VA and DOD sites. Although the data being exchanged were limited, implementing this interface is a milestone toward the long-term goal of modernized systems with interoperable electronic medical records.

While working on this long-term effort, the two departments also made progress in various near-term initiatives to exchange electronic medical information in their existing systems. The departments completed development of a system to allow the one-way transfer of health information from DOD to VA when service members leave the military. DOD has been using this system (the Federal Health Information Exchange or FHIE) to transfer information to VA since 2002. According to department officials, as of March 2007, over 184 million clinical messages on more than 3.8 million veterans had been transferred to the FHIE data repository, and VA had been given access to data for more than 681,000 separated service members and demobilized Reserve and National Guard members who had been deployed. Transfers are done in batches once a month, or weekly for veterans who have been referred to VA treatment facilities. According to a joint DOD/VA report,[35] FHIE has made a significant contribution to the delivery and continuity of care of separated service members as they transition to veteran status, as well as to the adjudication of disability claims.

In addition, two ongoing demonstration projects were successfully exchanging particular types of data at selected sites:

- The Laboratory Data Sharing Interface allows DOD and VA facilities serving the same geographic area to share laboratory resources. As

[35] December 2004 VA and DOD Joint Strategic Plan.

of May 2007, this capability had been deployed at 9 localities to communicate orders for lab tests and their results electronically and could be deployed at others if the need is demonstrated.

- The Bidirectional Health Information Exchange allows a real-time, two-way view of health data from existing systems.[36] As of May 2007, this system provided this capability (for outpatient data) to all VA sites and 25 DOD sites and (for certain inpatient discharge summary data)[37] to all VA sites and 5 DOD sites. Expanding this interface is the foundation of the departments' interim strategy to share information among their existing systems.

The two departments had also undertaken ad hoc activities to accelerate the transmission of health information on severely wounded patients from DOD to VA's four polytrauma centers. These centers care for veterans and service members with disabling injuries to more than one physical region or organ system. The ad hoc processes include manual workarounds such as scanning paper records and individually transmitting radiological images. Such processes were generally feasible only because the number of polytrauma patients was small (about 350 in all as of May 2007).

Through all these efforts, VA and DOD have achieved exchanges of health information. However, these exchanges are as yet limited, and it is not clear how they are to be integrated into an overall strategy toward achieving the departments' long-term goal of comprehensive, seamless exchange of health information. Significant work remains to be done for the departments to achieve their long-term goals, including agreeing to standards for the remaining categories of medical information, populating the data repositories with all this information, completing the development of their modernized systems, and transitioning from the legacy systems. In addition, the departments have not yet projected a completion date for the project as a whole. Consequently, it is

[36] DOD's Composite Health Care System (CHCS) and VA's VistA (Veterans Health Information Systems and Technology Architecture).

[37] Specifically, inpatient discharge summary data stored in VA's VistA and DOD's Clinical Information System (CIS), a commercial health information system customized for DOD.

essential for the departments to develop a comprehensive project plan to guide this effort to completion. In previous work, we have made numerous recommendations with regard to this effort, placing particular stress on the need for comprehensive planning.[38] VA and DOD have agreed with our recommendations, and have taken action to implement them. However, at the time of our May testimony, the two departments had not yet developed a comprehensive integrated project plan.

The need for such a comprehensive plan is further highlighted by the strategy announced by the two departments in January 2007: that is, to jointly develop a new inpatient medical record system. The departments have indicated that by adopting a joint solution, they could realize significant cost savings and make inpatient health care data immediately accessible to both departments. Incorporating this new strategy into the departments' ongoing efforts would be greatly facilitated by a comprehensive project plan.

In summary, effectively instituting the realignment is essential to ensuring that its IT programs achieve their objectives and that VA has a solid and sustainable approach to managing its IT investments. The department continues to work on improving such programs as information security and asset control, and it currently has many significant initiatives under way, for which substantial investments have been made. 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. However, until the department provides the foundation for its new IT management structure by carrying out its plans to establish a comprehensive set of improved management processes, the impact of this vital undertaking will be diminished. Implementation of the recommendations that we have

[38] GAO, *Computer-Based Patient Records: VA and DOD Made Progress, but Much Work Remains to Fully Share Medical Information*, GAO-05-1051T (Washington, D.C.: Sept. 28, 2005) and *Information Technology: VA and DOD Face Challenges in Completing Key Efforts*, GAO-06-905T (Washington, D.C.: June 22, 2006).

made in this area could play a significant role in resolving many of these concerns.

Mr. Chairman, this concludes my statement. I would be pleased to respond to any questions that you or other members of the committee may have at this time.

Contacts and Acknowledgements

For information about this testimony, please contact Valerie C. Melvin at (202) 512-6304 or melvinv@gao.gov. Key contributions to this testimony were made by Barbara Oliver, Assistant Director; Barbara Collier, B. Scott Pettis; J. Michael Resser; Eric Trout, and Charles Youman.

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

Key area	IT management process	Description
Enterprise management	Information technology (IT) strategy	Addressing 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	Defining a structure of relationships and processes to direct and control the IT endeavor.
	Risk management	Identifying potential events that may affect the organization and managing risk to be within acceptable levels so that reasonable assurance is provided regarding the achievement of organization objectives.
	Architecture management	Creating, maintaining, promoting, and governing the use of IT architecture models and standards across and within the change programs of an organization.
	Portfolio management	Assessing all applications, services, and IT projects that consume resources in order to understand their value to the IT organization.
	Security management	Managing the department's information security program, as mandated by the Federal Information Security Management Act (FISMA) of 2002.
	IT research and innovation	Generating ideas, evaluating and selecting ideas, developing and implementing innovations, and continuously recognizing innovators and learning from the experience.
	Project management	Planning, organizing, monitoring, and controlling all aspects of a project in a continuous process so that it achieves its objectives.
Business management	Stakeholder requirements management	Managing and prioritizing all requests for additional and new technology solutions arising from a customer's needs.
	Customer satisfaction management	Determining whether and how well customers are satisfied with the services, solutions, and offerings from the providers of IT.
	Financial management	Providing sound stewardship of the monetary resources of the organization.
	Service pricing and contract administration	Establishing 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	Enabling 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.
	Compliance management	Ensuring adherence with laws and regulations, internal policies and procedures, and stakeholder commitments.
	Asset management	Maintaining information regarding technology assets, included leased and purchased assets, licenses, and inventory.
	Workforce management	Enabling 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	Managing service-level agreements and performing 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	Ensuring that agreed-on IT services continue to support business requirements in the event of a disruption to the business.

Key area	IT management process	Description
	Supplier relationship management	Developing and exercising 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	Promoting an integrated approach to identifying, capturing, evaluating, categorizing, retrieving, and sharing all of an organization's information assets.
Business application management	Solution requirements	Translating 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	Creating a documented design from agreed-on solution requirements that describes the behavior of solution elements, the acceptance criteria, and agreed-to measurements.
	Solution build	Bringing together all the elements specified by a solution design via customization, configuration, and integration of created or acquired solution components.
	Solution test and acceptance	Validating that the solution components and integrated solutions conform to design specifications and requirements before deployment.
Infrastructure	Service execution	Addressing 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	Ensuring 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	Identifying and prioritizing infrastructure, service, business, and security events, and establishing the appropriate response to those events.
	Availability management	Planning, measuring, monitoring, and continuously striving to improve the availability of the IT infrastructure and supporting organization to ensure that agreed-on requirements are consistently met.
	Capacity management	Matching the capacity of the IT services and infrastructure to the current and future identified needs of the business.
	Facility management	Creating and maintaining a physical environment that houses IT resources and optimizes the capabilities and costs of that environment.
Service support	Change management	Managing the life cycle of a change request and activities that measure the effectiveness of the process as well as providing for its continued enhancement.
	Release management	Controlling 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	Identifying, controlling, maintaining, and verifying the versions of configuration items and their relationships in a logical model of the infrastructure and services.
	User contact management	Managing each user interaction with the provider of IT service throughout its life cycle.
	Incident management	Restoring 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	Resolving problems affecting the IT service, both reactively and proactively.

Source: GAO analysis of VA documentation.

(310911)

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